



EliteConnect™ Universal 2.4GHz/5GHz Wireless Dual-Band Outdoor Access Point/Bridge

The easy way to make all your network connections



38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

May 2005
Revision Number: R01
F1.1.2.5

Copyright

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2005 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

All rights reserved.

Trademarks:

SMC is a registered trademark; and EliteConnect is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:

http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968.

LIMITED WARRANTY

Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

- * SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

COMPLIANCES

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Warnings: 1. Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.
2. When connecting this device to a power outlet, connect the field ground lead on the tri-pole power plug to a valid earth ground line to prevent electrical hazards.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Wireless 5 GHz Band Statements:

As the SMC2888W access point/bridge can operate in the 5150-5250 MHz frequency band it is limited by the FCC, Industry Canada and some other countries to indoor use only so as to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

High power radars are allocated as primary users (meaning they have priority) of the 5250-5350 MHz and 5650-5850 MHz bands. These radars could cause interference and/or damage to the access point.

EC Conformance Declaration 0560

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Frutuós Gelabert 6-8, 2^a, 4^a,
08970 - Sant Joan Despí,
Barcelona, Spain.

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950 (IEC 60950) - Product Safety
- EN 301 893 - Technical requirements for 5 GHz radio equipment
- EN 300 328 - Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1 / EN 301 489-17 - EMC requirements for radio equipment

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

Note: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

- This device requires that the user or installer properly enter the current country of operation in the command line interface as described in the user guide, before operating this device.
- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other system. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.

- This device employs a radar detection feature required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
- The 5 GHz Turbo Mode feature is not allowed for operation in any European Community country. The current setting for this feature is found in the 5 GHz 802.11a Radio Settings Window as described in the user guide.
- The 5 GHz radio's Auto Channel Select setting described in the user guide must always remain enabled to ensure that automatic 5 GHz channel selection complies with European requirements. The current setting for this feature is found in the 5 GHz 802.11a Radio Settings Window as described in the user guide.
- This device is restricted to *indoor* use when operated in the European Community using the 5.15 - 5.35 GHz band: Channels 36, 40, 44, 48, 52, 56, 60, 64. See table below for allowed 5 GHz channels by country.
- This device may be operated *indoors or outdoors* in all countries of the European Community using the 2.4 GHz band: Channels 1 - 13, except where noted below.
 - In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
 - In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
 - In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7

Operation Using 5 GHz Channels in the European Community

The user/installer must use the provided configuration utility to check the current channel of operation and make necessary configuration changes to ensure operation occurs in conformance with European National spectrum usage laws as described below and elsewhere in this document.

Allowed 5GHz Channels in Each European Community Country		
Allowed Frequency Bands	Allowed Channel Numbers	Countries
5.15 - 5.25 GHz*	36, 40, 44, 48	Austria, Belgium
5.15 - 5.35 GHz*	36, 40, 44, 48, 52, 56, 60, 64	France, Switzerland, Liechtenstein
5.15 - 5.35* & 5.470 - 5.725 GHz	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Denmark, Finland, Germany, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, U.K.
5 GHz Operation Not Allowed	None	Greece

* Outdoor operation is not allowed using 5.15-5.35 GHz bands (Channels 36 - 64).

* Currently channels 36-64 are unavailable for use either indoors or outdoors.

Declaration of Conformity in Languages of the European Community

English	Hereby, SMC Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja SMC Networks vakuuttaa täten että Radio LAN device tyypinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart SMC Networks dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze SMC Networks dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente SMC Networks déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
Swedish	Härmed intygar SMC Networks att denna Radio LAN device står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede SMC Networks erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
German	Hiermit erklärt SMC Networks, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW) Hiermit erklärt SMC Networks die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	Με την παρούσα SMC Networks δηλώνει ότι radio LAN device συμμορφώνεται προς τις ουσιαστικές απαιτήσεις και τις λοιπές σχετικές διατάξεις της οδηγίας 1999/5/εκ

Italian	Con la presente SMC Networks dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente SMC Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Portuguese	SMC Networks declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

Safety Compliance

Power Cord Safety

Please read the following safety information carefully before installing the wireless access point:

WARNING: Installation and removal of the unit must be carried out by qualified personnel only.

- The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.
- Do not connect the unit to an A.C. outlet (power supply) without an earth (ground) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.
- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

France and Peru only

This unit cannot be powered from IT[†] supplies. If your supplies are of IT type, this unit must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to earth (ground).

[†] Impédance à la terre

Important! Before making connections, make sure you have the correct cord set.
Check it (read the label on the cable) against the following:

Power Cord Set	
U.S.A. and Canada	The cord set must be UL-approved and CSA certified.
	The minimum specifications for the flexible cord are: - No. 18 AWG - not longer than 2 meters, or 16 AWG. - Type SV or SJ - 3-conductor
	The cord set must have a rated current capacity of at least 10 A
	The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15P (15 A, 250 V) configuration.
Denmark	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
Switzerland	The supply plug must comply with SEV/ASE 1011.
U.K.	The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5 A fuse which complies with BS1362.
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
Europe	The supply plug must comply with CEE7/7 ("SCHUKO").
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
	IEC-320 receptacle.

Veillez lire à fond l'information de la sécurité suivante avant d'installer le wireless access point:

AVERTISSEMENT: L'installation et la dépose de ce groupe doivent être confiés à un personnel qualifié.

- Ne branchez pas votre appareil sur une prise secteur (alimentation électrique) lorsqu'il n'y a pas de connexion de mise à la terre (mise à la masse).
- Vous devez raccorder ce groupe à une sortie mise à la terre (mise à la masse) afin de respecter les normes internationales de sécurité.
- Le coupleur d'appareil (le connecteur du groupe et non pas la prise murale) doit respecter une configuration qui permet un branchement sur une entrée d'appareil EN 60320/IEC 320.
- La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.
- L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme IEC 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.

France et Pérou uniquement:

Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse).

Cordon électrique - Il doit être agréé dans le pays d'utilisation	
Etats-Unis et Canada:	Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA.
	Les spécifications minimales pour un câble flexible sont AWG No. 18, ou AWG No. 16 pour un câble de longueur inférieure à 2 mètres. - type SV ou SJ - 3 conducteurs
	Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A.
	La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V).
Danemark:	La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a.

Cordon électrique - Il doit être agréé dans le pays d'utilisation	
Suisse:	La prise mâle d'alimentation doit respecter la norme SEV/ASE 1011.
Europe	La prise secteur doit être conforme aux normes CEE 7/7 ("SCHUKO") LE cordon secteur doit porter la mention <HAR> ou <BASEC> et doit être de type HO3VVF3GO.75 (minimum).

Bitte unbedingt vor dem Einbauen des Access Point die folgenden Sicherheitsanweisungen durchlesen (Germany):

WARNUNG: Die Installation und der Ausbau des Geräts darf nur durch Fachpersonal erfolgen.

- Das Gerät sollte nicht an eine ungeerdete Wechselstromsteckdose angeschlossen werden.
- Das Gerät muß an eine geerdete Steckdose angeschlossen werden, welche die internationalen Sicherheitsnormen erfüllt.
- Der Gerätestecker (der Anschluß an das Gerät, nicht der Wandsteckdosenstecker) muß einen gemäß EN 60320/IEC 320 konfigurierten Geräteeingang haben.
- Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.
- Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur

COMPLIANCES

gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.

Stromkabel. Dies muss von dem Land, in dem es benutzt wird geprüft werden:	
U.S.A und Kanada	Der Cord muß das UL geprüft und war das CSA beglaubigt.
	Das Minimum spezifikation für der Cord sind: - Nu. 18 AWG - nicht mehr als 2 meter, oder 16 AWG. - Der typ SV oder SJ - 3-Leiter
	Der Cord muß haben eine strombelastbarkeit aus wenigstens 10 A
	Dieser Stromstecker muß hat einer erdschluss mit der typ NEMA 5-15P (15A, 125V) oder NEMA 6-15P (15A, 250V) konfiguration.
Danemark	Dieser Stromstecker muß die ebene 107-2-D1, der standard DK2-1a oder DK2-5a Bestimmungen einhalten.
Schweiz	Dieser Stromstecker muß die SEV/ASE 1011 Bestimmungen einhalten.
Europe	Das Netzkabel muß vom Typ HO3VVF3GO.75 (Mindestanforderung) sein und die Aufschrift <HAR> oder <BASEC> tragen. Der Netzstecker muß die Norm CEE 7/7 erfüllen ("SCHUKO").

TABLE OF CONTENTS

1	Introduction	1-1
	Package Checklist	1-2
	Hardware Description	1-4
	Integrated High-Gain Antenna	1-5
	External Antenna Options	1-5
	Ethernet Port	1-5
	Power Injector Module	1-6
	Receive Signal Strength Indicator (RSSI)	
	BNC Connector	1-7
	Grounding Point	1-7
	Wall- and Pole-Mounting Bracket Kits	1-7
	System Configuration	1-8
	Features and Benefits	1-9
	System Defaults	1-10
2	Network Configuration	2-1
	Access Point Topologies	2-1
	Ad Hoc Wireless LAN (no Access Point or Bridge)	2-2
	Infrastructure Wireless LAN	2-3
	Infrastructure Wireless LAN for Roaming Wireless PCs	2-4
	Bridge Link Topologies	2-5
	Point-to-Point Configuration	2-6
	Point-to-Multipoint Configuration	2-6
3	Bridge Link Planning	3-1
	Radio Path Planning	3-1
	Antenna Height	3-3
	Antenna Position and Orientation	3-5
	Radio Interference	3-6
	Weather Conditions	3-7
	Ethernet Cabling	3-8
	Grounding	3-8
4	Hardware Installation	4-1
	Testing Basic Link Operation	4-2
	Mount the Unit	4-2
	Using the Pole-Mounting Bracket	4-2
	Using the Wall-Mounting Bracket	4-4

TABLE OF CONTENTS

Connect External Antennas	4-5
Connect Cables to the Unit	4-7
Connect the Power Injector	4-7
Align Antennas	4-9
5 Initial Configuration	5-1
Initial Setup through the CLI	5-2
Initial Configuration Steps	5-2
Using the Web-based Management Setup Wizard	5-4
6 System Configuration	6-1
Advanced Configuration	6-3
System Identification	6-4
TCP / IP Settings	6-7
Radius	6-10
PPPoE Settings	6-13
Authentication	6-16
Filter Control	6-26
SNMP	6-30
Administration	6-33
System Log	6-38
Wireless Distribution System (WDS)	6-43
Bridge	6-45
Spanning Tree Protocol (STP)	6-47
RSSI	6-54
Radio Interface	6-56
Radio Settings A (802.11a)	6-57
Radio Settings G (802.11g)	6-63
Security (Bridge Mode)	6-66
Security (Access Point Mode)	6-72
Status Information	6-87
AP Status	6-87
Station Status	6-90
Event Logs	6-92
7 Command Line Interface	7-1
Using the Command Line Interface	7-1
Accessing the CLI	7-1
Telnet Connection	7-1

Entering Commands	7-3
Keywords and Arguments	7-3
Minimum Abbreviation	7-3
Command Completion	7-3
Getting Help on Commands	7-4
Partial Keyword Lookup	7-5
Negating the Effect of Commands	7-5
Using Command History	7-5
Understanding Command Modes	7-6
Exec Commands	7-6
Configuration Commands	7-7
Command Line Processing	7-8
Command Groups	7-9
General Commands	7-10
configure	7-10
end	7-11
exit	7-11
ping	7-12
reset	7-13
show history	7-14
show line	7-14
System Management Commands	7-15
country	7-16
prompt	7-18
system name	7-19
username	7-19
password	7-20
ip http port	7-20
ip http server	7-21
show system	7-22
show version	7-23
System Logging Commands	7-23
logging on	7-24
logging host	7-24
logging console	7-25
logging level	7-25
logging facility-type	7-26
show logging	7-27

TABLE OF CONTENTS

System Clock Commands	7-28
ntp-server ip	7-29
ntp-server enable	7-30
ntp-server date-time	7-31
ntp-server daylight-saving	7-31
ntp-server timezone	7-32
show ntp	7-33
SNMP Commands	7-34
snmp-server community	7-34
snmp-server contact	7-35
snmp-server enable server	7-36
snmp-server host	7-37
snmp-server location	7-38
show snmp	7-39
Flash/File Commands	7-39
bootfile	7-40
copy	7-41
delete	7-42
dir	7-43
RADIUS Client	7-45
radius-server address	7-45
radius-server port	7-46
radius-server key	7-47
radius-server retransmit	7-47
radius-server timeout	7-48
show radius	7-48
Authentication	7-49
802.1x	7-51
802.1x broadcast-key-refresh-rate	7-52
802.1x session-key-refresh-rate	7-53
802.1x session-timeout	7-54
802.1x supplicant	7-55
address filter default	7-56
address filter entry	7-57
address filter delete	7-58
mac-authentication server	7-59
mac-authentication session-timeout	7-60
show authentication	7-60

TABLE OF CONTENTS

WDS Commands	7-61
wds channel	7-62
wds mac-address	7-62
wds enable	7-63
show wds	7-64
Bridge Commands	7-65
bridge timeout	7-66
bridge stp-bridge spanning-tree	7-66
bridge stp-bridge forward-time	7-67
bridge stp-bridge hello-time	7-68
bridge stp-bridge max-age	7-69
bridge stp-bridge priority	7-70
bridge stp-port path-cost	7-71
bridge stp-port priority	7-72
bridge stp-port portfast	7-73
bridge stp-port spanning-disabled	7-74
show bridge	7-75
Filtering Commands	7-76
filter local-bridge	7-76
filter ap-manage	7-77
filter ethernet-type enable	7-78
filter ethernet-type protocol	7-79
show filters	7-80
PPPoE Commands	7-80
ip pppoe	7-81
pppoe ip allocation mode	7-82
pppoe ipcp dns	7-83
pppoe lcp echo-interval	7-84
pppoe lcp echo-failure	7-85
pppoe local ip	7-86
pppoe remote ip	7-86
pppoe username	7-87
pppoe password	7-88
pppoe service-name	7-89
pppoe restart	7-89
show pppoe	7-90
Ethernet Interface Commands	7-91
interface ethernet	7-91

TABLE OF CONTENTS

dns server	7-92
ip address	7-93
ip dhcp	7-94
shutdown	7-95
show interface ethernet	7-96
Wireless Interface Commands	7-97
interface wireless	7-99
description	7-99
ssid	7-100
closed-system	7-101
speed	7-101
channel	7-102
turbo	7-103
beacon-interval	7-104
dtim-period	7-104
fragmentation-length	7-105
rts-threshold	7-106
transmit-power	7-107
max-association	7-108
authentication	7-109
encryption	7-110
key	7-112
transmit-key	7-113
multicast-cipher	7-114
wpa-clients	7-116
wpa-mode	7-117
wpa-preshared-key	7-118
wpa-psk-type	7-119
shutdown	7-120
show interface wireless	7-120
show station	7-121
IAPP Commands	7-122
iapp	7-122
VLAN Commands	7-123
vlan	7-124
native-vlanid	7-125

A	Troubleshooting	A-1
B	Specifications	B-1
	General Specifications	B-1
	Antenna Specifications	B-4
	17 dBi Integrated Panel	B-4
C	Cables and Pinouts	C-1
	Twisted-Pair Cable Assignments	C-1
	10/100BASE-TX Pin Assignments	C-2
	Straight-Through Wiring	C-3
	Crossover Wiring	C-3
	8-Pin DIN Connector Pinout	C-4
	8-Pin DIN to RJ-45 Cable Wiring	C-5

Glossary

Index

TABLE OF CONTENTS

Chapter 1

Introduction

The SMC EliteConnect Universal 2.4GHz/5GHz Wireless Dual-Band Outdoor Access Point/Bridge system consists of two models that provide point-to-point or point-to-multipoint bridge links between remote Ethernet LANs, and wireless access point services for clients in the local LAN area:

- **SMC2888W-S** – Includes an integrated high-gain antenna for the 802.11a radio and is designed to operate as a “Slave” bridge in point-to-multipoint configurations, or provide a high-speed point-to-point wireless link between two sites. The 802.11b/g radio requires an external antenna option.
- **SMC2888W-M** – Provides only external antenna options and is designed to operate as the “Master” bridge in point-to-multipoint configurations, supporting wireless bridge connections to as many as 16 SMC2888W-S Slave units.

Each model is housed in a weatherproof enclosure for mounting outdoors and includes its own brackets for attaching to a wall, pole, radio mast, or tower structure. The unit is powered through its Ethernet cable connection from a power injector module that is installed indoors.

The wireless bridge system offers a fast, reliable, and cost-effective solution for connectivity between remote Ethernet wired LANs or to provide Internet access to an isolated site. The system is also easy to install and operate, ideal for situations where a wired link may be difficult or expensive to deploy. The wireless bridge connection provides data rates of up to 108 Mbps.

Introduction

In addition, both wireless bridge models offer full network management capabilities through an easy-to-use web interface, a command-line interface, and support for Simple Network Management Protocol (SNMP) tools.

Radio Characteristics – The IEEE 802.11a and 802.11g standards use a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). The 802.11a standard operates in the 5 GHz Unlicensed National Information Infrastructure (UNII) band, and the 802.11g standard in the 2.4 GHz band.

IEEE 802.11g includes backward compatibility with the IEEE 802.11b standard. IEEE 802.11b also operates at 2.4 GHz, but uses Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) modulation technology to achieve a communication rate of up to 11 Mbps.

The wireless bridge provides a 54 Mbps half-duplex connection for each active channel (up to 108 Mbps in turbo mode on the 802.11a interface).

Package Checklist

The Dual-band Outdoor Access Point / Bridge package includes:

- One EliteConnect Universal 2.4GHz/5GHz Wireless Dual-Band Outdoor Access Point/Bridge (SMC2888W-S or SMC2888W-M)
- One Category 5 network cable, length 164 ft (50 m)
- One power injector module and power cord

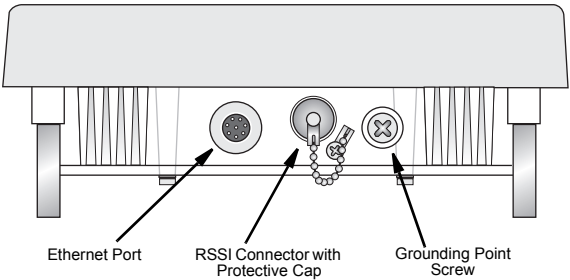
Package Checklist

- Outdoor pole-mounting bracket kit
- Outdoor wall-mounting bracket kit
- This User Guide

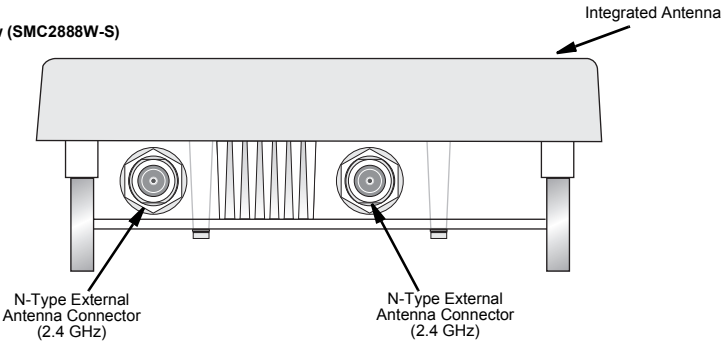
Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

Hardware Description

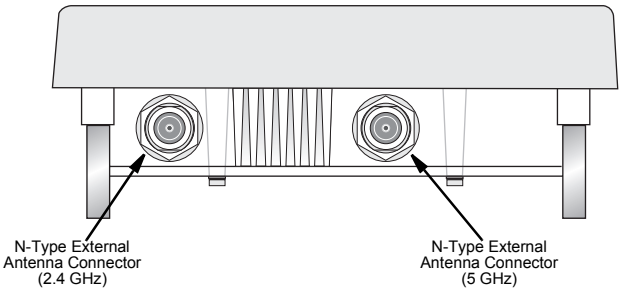
Bottom View



Top View (SMC2888W-S)



Top View (SMC2888W-M)



Integrated High-Gain Antenna

The SMC2888W-S wireless bridge includes an integrated high-gain (17 dBi) flat-panel antenna for 5 GHz operation.

External Antenna Options

The SMC2888W-M Master bridge unit does not include an integrated antenna, but provides various external antenna options for both 5 GHz and 2.4 GHz operation. In a point-to-multipoint configuration, an external high-gain omnidirectional, sector, or high-gain panel antenna can be attached to communicate with bridges spread over a wide area.

External antennas connect to the N-type RF connectors on the wireless bridge using the provided coaxial cables.

Ethernet Port

The wireless bridge has one 10BASE-T/100BASE-TX 8-pin DIN port that connects to the power injector module using the included Ethernet cable. The Ethernet port connection provides power to the wireless bridge as well as a data link to the local network.

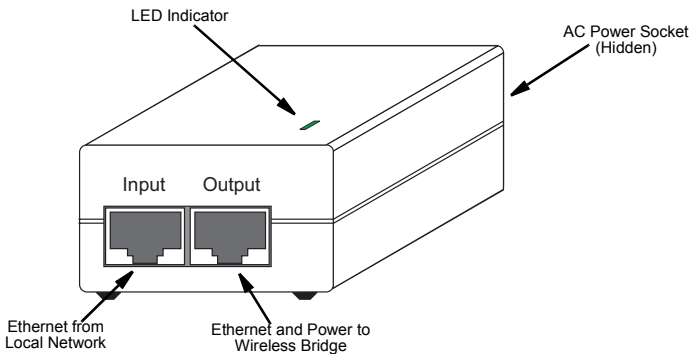
The wireless bridge appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to the remote end of the wireless bridge link.

Note: The power injector module does not support Power over Ethernet (PoE) based on the IEEE 802.3af standard. The wireless bridge unit must always be powered on by being connected to the power injector module.

Power Injector Module

The wireless bridge receives power through its network cable connection using power-over-Ethernet technology. A power injector module is included in the wireless bridge package and provides two RJ-45 Ethernet ports, one for connecting to the wireless bridge (Output), and the other for connecting to a local LAN switch (Input).

The Input port uses an MDI (i.e., internal straight-through) pin configuration. You can therefore use straight-through twisted-pair cable to connect this port to most network interconnection devices such as a switch or router that provide MDI-X ports. However, when connecting the access point to a workstation or other device that does not have MDI-X ports, you must use crossover twisted-pair cable.



The wireless bridge does not have a power switch. It is powered on when its Ethernet port is connected to the power injector module, and the power injector module is connected to an AC power source. The power injector includes one LED indicator that turns on when AC power is applied.

The power injector module automatically adjusts to any AC voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

Warning: The power injector module is designed for indoor use only. Never mount the power injector outside with the wireless bridge unit.

Receive Signal Strength Indicator (RSSI) BNC Connector

The RSSI connector provides an output voltage that is proportional to the received radio signal strength. A DC voltmeter can be connected this port to assist in aligning the antennas at both ends of a wireless bridge link.

Grounding Point

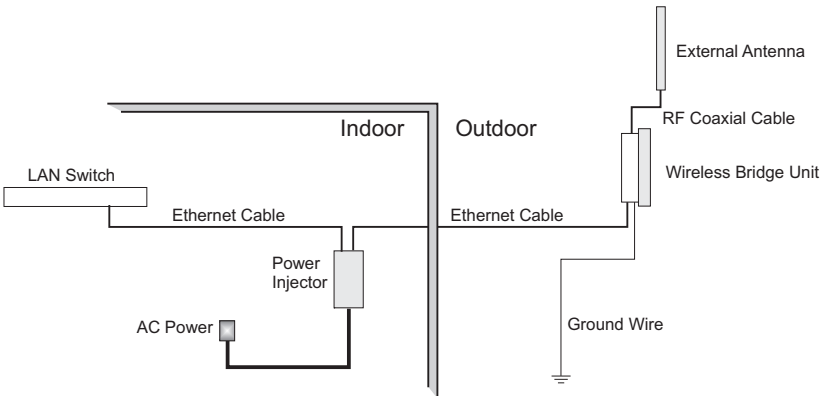
Even though the wireless bridge includes its own built-in lightning protection, it is important that the unit is properly connected to ground. A grounding screw is provided for attaching a ground wire to the unit.

Wall- and Pole-Mounting Bracket Kits

The wireless bridge includes bracket kits that can be used to mount the bridge to a wall, pole, radio mast, or part of a tower structure.

System Configuration

At each location where a unit is installed, it must be connected to the local network using the power injector module. The following figure illustrates the system component connections.



Features and Benefits

- SMC2888W-S Slave units support a 5 GHz high-gain 17 dBi antenna
- SMC2888W-M Master units support 5 GHz point-to-multipoint links using various external antenna options
- Both SMC2888W-S and SMC2888W-M units also support access point services for the 5 GHz and 2.4 GHz radios using various external antenna options
- Maximum data rate up to 108 Mbps on the 802.11a (5 GHz) radio
- Outdoor weatherproof design
- IEEE 802.11a and 802.11b/g compliant
- Local network connection via 10/100 Mbps Ethernet port
- Powered through its Ethernet cable connection to the power injector module
- Includes wall- and pole-mount brackets
- Security through 64/128/152-bit Wired Equivalent Protection (WEP) or 128-bit Advanced Encryption Standard (AES) encryption, and WiFi Protected Areas (WPA)
- Scans all available channels and selects the best channel and data rate based on the signal-to-noise ratio
- Manageable through an easy-to-use web-browser interface, command line (via Telnet), or SNMP network management tools

System Defaults

The following table lists some of the wireless bridge's basic system defaults. To reset the bridge defaults, use the CLI command "reset configuration" from the Exec level prompt.

Feature	Parameter	Default
Identification	System Name	Dual Band Outdoor AP
Administration	User Name	admin
	Password	smcadmin
General	HTTP Server	Enabled
	HTTP Server Port	80
TCP/IP	IP Address	DHCP
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	Primary DNS IP	0.0.0.0
	Secondary DNS IP	0.0.0.0
VLANs	Status	Disabled
	Native VLAN ID	1
Filter Control	Ethernet Type	Disabled

System Defaults

Feature	Parameter	Default
SNMP	Status	Enabled
	Location	<i>null</i>
	Contact	Contact
	Community (Read Only)	Public
	Community (Read/Write)	Private
	Traps	Enabled
	Trap Destination IP Address	<i>null</i>
	Trap Destination Community Name	Public
System Logging	Syslog	Disabled
	Logging Host	Disabled
	Logging Console	Disabled
	IP Address / Host Name	0.0.0.0
	Logging Level	Informational
	Logging Facility Type	16
Spanning Tree	Status	Enabled
Ethernet Interface	Speed and Duplex	Auto
WDS Bridging	Outdoor Bridge Band	A (802.11a)

Introduction

Feature	Parameter	Default
Wireless Interface 802.11a	Status	Enabled
	SSID	SMC
	Turbo Mode	Disabled
	Radio Channel	Default to first channel
	Auto Channel Select	Enabled
	Transmit Power	Full
	Maximum Data Rate	54 Mbps
	Beacon Interval	100 TUs
	Data Beacon Rate (DTIM Interval)	2 beacons
	RTS Threshold	2347 bytes
Wireless Security 802.11a	Authentication Type	Open System
	AES Encryption	Disabled
	WEP Encryption	Disabled
	WEP Key Length	128 bits
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	<i>null</i>

System Defaults

Feature	Parameter	Default
Wireless Interface 802.11b/g	Status	Enabled
	SSID	SMC
	Radio Channel	Default to first channel
	Auto Channel Select	Enabled
	Transmit Power	Full
	Maximum Data Rate	54 Mbps
	Beacon Interval	100 TUs
	Data Beacon Rate (DTIM Interval)	2 beacons
	RTS Threshold	2347 bytes
Wireless Security 802.11b/g	Authentication Type	Open System
	AES Encryption	Disabled
	WEP Encryption	Disabled
	WEP Key Length	128 bits
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	<i>null</i>

Introduction

Chapter 2

Network Configuration

The Dual-band Outdoor Access Point / Bridge system provides access point or bridging services through either the 5 GHz or 2.4 GHz radio interfaces.

The wireless bridge units can be used just as normal 802.11a/b/g access points connected to a local wired LAN, providing connectivity and roaming services for wireless clients in an outdoor area. Units can also be used purely as bridges connecting remote LANs. Alternatively, you can employ both access point and bridging functions together, offering a flexible and convenient wireless solution for many applications.

This chapter describes the role of wireless bridge in various wireless network configurations.

Access Point Topologies

Wireless networks support a stand-alone wireless configuration as well as an integrated configuration with 10/100 Mbps Ethernet LANs.

Wireless network cards, adapters, and access points can be configured as:

- Ad hoc for departmental, SOHO, or enterprise LANs
- Infrastructure for wireless LANs
- Infrastructure wireless LAN for roaming wireless PCs

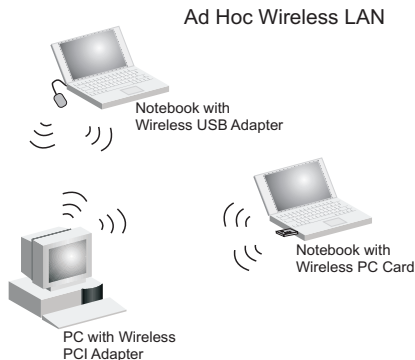
Network Configuration

The 802.11b and 802.11g frequency band, which operates at 2.4 GHz, can easily encounter interference from other 2.4 GHz devices, such as other 802.11b or g wireless devices, cordless phones and microwave ovens. If you experience poor wireless LAN performance, try the following measures:

- Limit any possible sources of radio interference within the service area
- Increase the distance between neighboring access points
- Increase the channel separation of neighboring access points (e.g., up to 3 channels of separation for 802.11b or up to 5 channels for 802.11g)

Ad Hoc Wireless LAN (no Access Point or Bridge)

An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected through radio signals as an independent wireless LAN. Computers in a specific ad hoc wireless LAN must therefore be configured to the same radio channel.

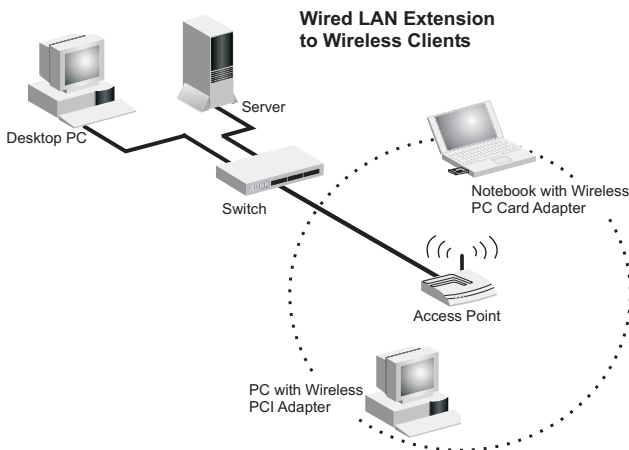


Infrastructure Wireless LAN

The access point function of the wireless bridge provides access to a wired LAN for 802.11a/b/g wireless workstations. An integrated wired/wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users and an access point that is directly connected to the wired LAN. Each wireless PC in a BSS can connect to any computer in its wireless group or access other computers or network resources in the wired LAN infrastructure through the access point.

The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signals through one or more access points.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure.

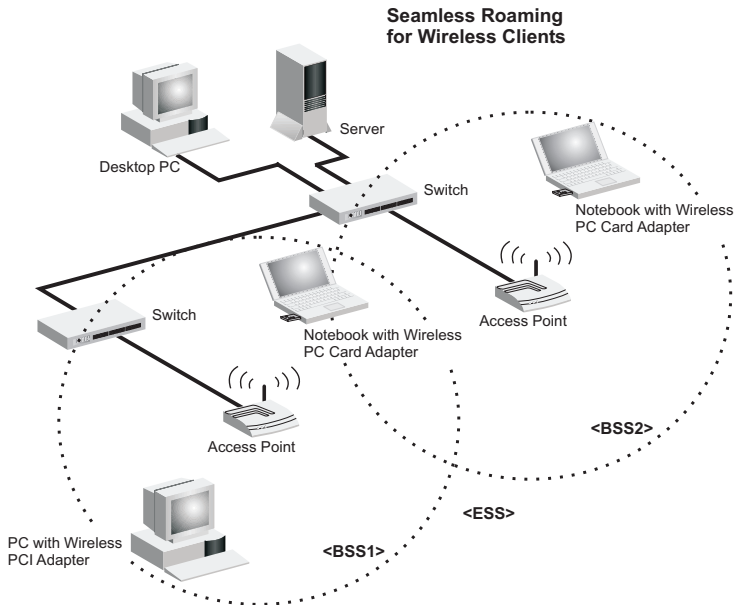


Infrastructure Wireless LAN for Roaming Wireless PCs

The Basic Service Set (BSS) defines the communications domain for each access point and its associated wireless clients. The BSS ID is a 48-bit binary number based on the access point's wireless MAC address, and is set automatically and transparently as clients associate with the access point. The BSS ID is used in frames sent between the access point and its clients to identify traffic in the service area.

The BSS ID is only set by the access point, never by its clients. The clients only need to set the Service Set Identifier (SSID) that identifies the service set provided by one or more access points. The SSID can be manually configured by the clients, can be detected in an access point's beacon, or can be obtained by querying for the identity of the nearest access point. For clients that do not need to roam, set the SSID for the wireless card to that used by the access point to which you want to connect.

A wireless infrastructure can also support roaming for mobile workers. More than one access point can be configured to create an Extended Service Set (ESS). By placing the access points so that a continuous coverage area is created, wireless users within this ESS can roam freely. All wireless network card adapters and wireless access points within a specific ESS must be configured with the same SSID.



Bridge Link Topologies

The IEEE 802.11 standard defines a Wireless Distribution System (WDS) for bridge connections between BSS areas (access points). The outdoor wireless bridge uses WDS to forward traffic on links between units. Up to 16 WDS links can be specified for a SMC2888W-M unit, which acts as the “Master” in the wireless bridge network. SMC2888W-S Slave units support only one WDS link, which must be to the network’s master unit.

The SMC2888W-M and SMC2888W-S support WDS bridge links on either the 5 GHz (802.11a) or 2.4 GHz (802.11b/g) bands and can be used with various external antennas to offer flexible deployment options.

Network Configuration

Note: The external antennas offer longer range options using the 5 GHz radio, which makes this interface more suitable for bridge links.

When using WDS on a radio band, only wireless bridge units can associate to each other. Wireless clients can only associate with the wireless bridge using a radio band set to access point mode.

Point-to-Point Configuration

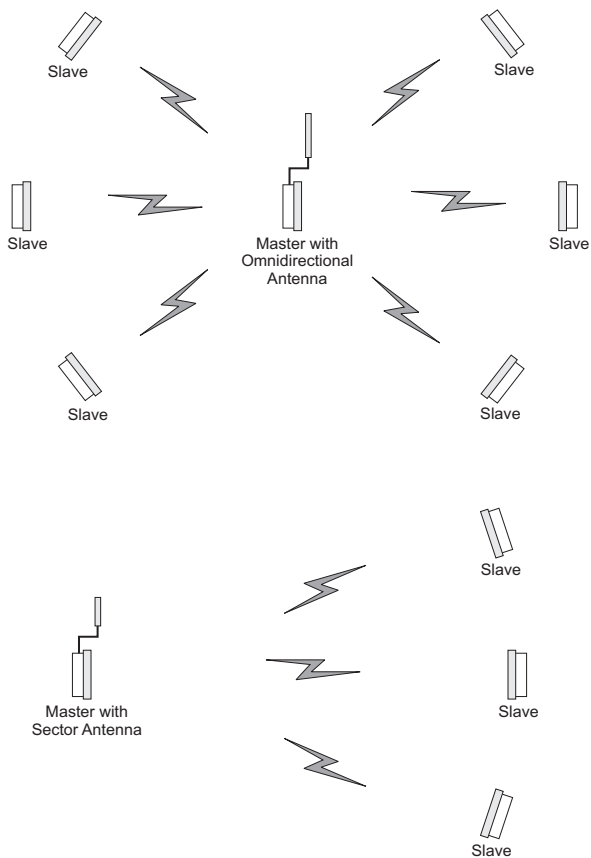
Two SMC2888W-S bridges can form a wireless point-to-point link using their 5 GHz (802.11a) integrated antennas.



Point-to-Multipoint Configuration

A SMC2888W-M wireless bridge can use an omnidirectional or sector antenna to connect to as many as 16 bridges in a point-to-multipoint configuration. There can only be one SMC2888W-M “Master” unit in the wireless bridge network, all other bridges must be SMC2888W-S “Slave” units.

Bridge Link Topologies



Network Configuration

Chapter 3

Bridge Link Planning

The SMC Dual-band Outdoor Access Point / Bridge supports fixed point-to-point or point-to-multipoint wireless links. A single link between two points can be used to connect a remote site to larger core network. Multiple bridge links can provide a way to connect widespread Ethernet LANs.

For each link in a wireless bridge network to be reliable and provide optimum performance, some careful site planning is required. This chapter provides guidance and information for planning your wireless bridge links.

Note: The planning and installation of the wireless bridge requires professional personnel that are trained in the installation of radio transmitting equipment. The user is responsible for compliance with local regulations concerning items such as antenna power, use of lightning arrestors, grounding, and radio mast or tower construction. Therefore, it is recommended to consult a professional contractor knowledgeable in local radio regulations prior to equipment installation.

Radio Path Planning

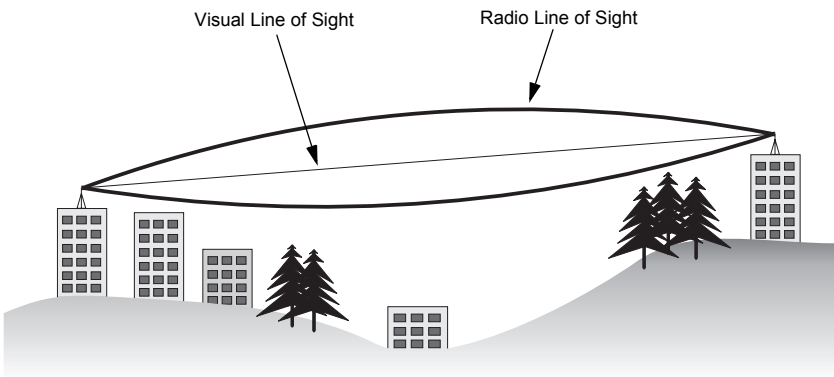
Although the wireless bridge uses IEEE 802.11a radio technology, which is capable of reducing the effect of multipath signals due to obstructions, the wireless bridge link requires a “radio line-of-sight” between the two antennas for optimum performance.

The concept of radio line-of-sight involves the area along a radio link path through which the bulk of the radio signal power travels.

Bridge Link Planning

This area is known as the first Fresnel Zone of the radio link. For a radio link not to be affected by obstacles along its path, no object, including the ground, must intrude within 60% of the first Fresnel Zone.

The following figure illustrates the concept of a good radio line-of-sight.



If there are obstacles in the radio path, there may still be a radio link but the quality and strength of the signal will be affected. Calculating the maximum clearance from objects on a path is important as it directly affects the decision on antenna placement and height. It is especially critical for long-distance links, where the radio signal could easily be lost.

When planning the radio path for a wireless bridge link, consider these factors:

- Avoid any partial line-of-sight between the antennas.
- Be cautious of trees or other foliage that may be near the path, or may grow and obstruct the path.

- Be sure there is enough clearance from buildings and that no building construction may eventually block the path.
- Check the topology of the land between the antennas using topographical maps, aerial photos, or even satellite image data (software packages are available that may include this information for your area).
- Avoid a path that may incur temporary blockage due to the movement of cars, trains, or aircraft.

Antenna Height

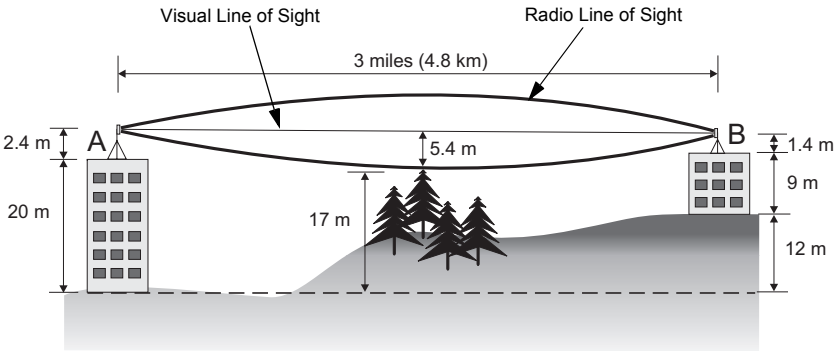
A reliable wireless link is usually best achieved by mounting the antennas at each end high enough for a clear radio line of sight between them. The minimum height required depends on the distance of the link, obstacles that may be in the path, topology of the terrain, and the curvature of the earth (for links over 3 miles).

For long-distance links, a mast or pole may need to be constructed to attain the minimum required height. Use the following table to estimate the required minimum clearance above the ground or path obstruction (for 5 GHz bridge links).

Bridge Link Planning

Total Link Distance	Max Clearance for 60% of First Fresnel Zone at 5.8 GHz	Approximate Clearance for Earth Curvature	Total Clearance Required at Mid-point of Link
0.25 mile (402 m)	4.5 ft (1.4 m)	0	4.5 ft (1.4 m)
0.5 mile (805 m)	6.4 ft (1.95 m)	0	6.4 ft (1.95 m)
1 mile (1.6 km)	9 ft (2.7 m)	0	9 ft (2.7 m)
2 miles (3.2 km)	12.7 ft (3.9 m)	0	12.7 ft (3.9 m)
3 miles (4.8 km)	15.6 ft (4.8 m)	1.8 ft (0.5 m)	17.4 ft (5.3 m)
4 miles (6.4 km)	18 ft (5.5 m)	3.2 ft (1.0 m)	21.2 ft (6.5 m)
5 miles (8 km)	20 ft (6.1 m)	5 ft (1.5 m)	25 ft (7.6 m)
7 miles (11.3 km)	24 ft (7.3 m)	9.8 ft (3.0 m)	33.8 ft (10.3 m)
9 miles (14.5 km)	27 ft (8.2 m)	16 ft (4.9 m)	43 ft (13.1 m)
12 miles (19.3 km)	31 ft (9.5 m)	29 ft (8.8 m)	60 ft (18.3 m)
15 miles (24.1 km)	35 ft (10.7 m)	45 ft (13.7 m)	80 ft (24.4 m)
17 miles (27.4 km)	37 ft (11.3 m)	58 ft (17.7 m)	95 ft (29 m)

Note that to avoid any obstruction along the path, the height of the object must be added to the minimum clearance required for a clear radio line-of-sight. Consider the following simple example, illustrated in the figure below.



A wireless bridge link is deployed to connect building A to a building B, which is located three miles (4.8 km) away. Mid-way between the two buildings is a small tree-covered hill. From the above table it can be seen that for a three-mile link, the object clearance required at the mid-point is 5.3 m (17.4 ft). The tree-tops on the hill are at an elevation of 17 m (56 ft), so the antennas at each end of the link need to be at least 22.3 m (73 ft) high. Building A is six stories high, or 20 m (66 ft), so a 2.3 m (7.5 ft) mast or pole must be constructed on its roof to achieve the required antenna height. Building B is only three stories high, or 9 m (30 ft), but is located at an elevation that is 12 m (39 ft) higher than building A. To mount an antenna at the required height on building B, a mast or pole of only 1.3 m (4.3 ft) is needed.

Warning: Never construct a radio mast, pole, or tower near overhead power lines.

Note: Local regulations may limit or prevent construction of a high radio mast or tower. If your wireless bridge link requires a high radio mast or tower, consult a professional contractor for advice.

Antenna Position and Orientation

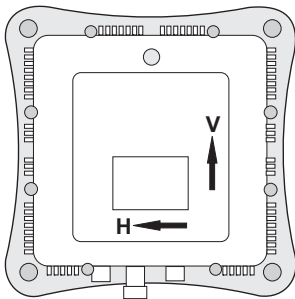
Once the required antenna height has been determined, other factors affecting the precise position of the wireless bridge must be considered:

- Be sure there are no other radio antennas within 2 m (6 ft) of the wireless bridge
- Place the wireless bridge away from power and telephone lines
- Avoid placing the wireless bridge too close to any metallic reflective surfaces, such as roof-installed air-conditioning equipment, tinted windows, wire fences, or water pipes

Bridge Link Planning

- The wireless bridge antennas at both ends of the link must be positioned with the same polarization direction, either horizontal or vertical

Antenna Polarization — The wireless bridge's integrated antenna sends a radio signal that is polarized in a particular direction. The antenna's receive sensitivity is also higher for radio signals that have the same polarization. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction. The antenna polarization is marked on the wireless bridge, as indicated in the following figure.



Radio Interference

The avoidance of radio interference is an important part of wireless link planning. Interference is caused by other radio transmissions using the same or an adjacent channel frequency. You should first scan your proposed site using a spectrum analyzer to determine if there are any strong radio signals using the 802.11a channel frequencies. Always use a channel frequency that is furthest away from another signal.

If radio interference is still a problem with your wireless bridge link, changing the antenna polarization direction may improve the situation.

Weather Conditions

When planning wireless bridge links, you must take into account any extreme weather conditions that are known to affect your location. Consider these factors:

- **Temperature** — The wireless bridge is tested for normal operation in temperatures from -33°C to 55°C. Operating in temperatures outside of this range may cause the unit to fail.
- **Wind Velocity** — The wireless bridge can operate in winds up to 90 MPH and survive higher wind speeds up to 125 MPH. You must consider the known maximum wind velocity and direction at the site and be sure that any supporting structure, such as a pole, mast, or tower, is built to withstand this force.
- **Lightning** — The wireless bridge includes its own built-in lightning protection. However, you should make sure that the unit, any supporting structure, and cables are all properly grounded. Additional protection using lightning rods, lightning arrestors, or surge suppressors may also be employed.
- **Rain** — The wireless bridge is weatherproofed against rain. Also, prolonged heavy rain has no significant effect on the radio signal. However, it is recommended to apply weatherproof sealing tape around the Ethernet port and antenna connectors for extra protection. If moisture enters a connector, it may cause a degradation in performance or even a complete failure of the link.
- **Snow and Ice** — Falling snow, like rain, has no significant effect on the radio signal. However, a build up of snow or ice on antennas may cause the link to fail. In this case, the snow or ice has to be cleared from the antennas to restore operation of the link.

Ethernet Cabling

When a suitable antenna location has been determined, you must plan a cable route from the wireless bridge outdoors to the power injector module indoors. Consider these points:

- The Ethernet cable length should never be longer than 100 m (328 ft)
- Determine a building entry point for the cable
- Determine if conduits, bracing, or other structures are required for safety or protection of the cable
- For lightning protection at the power injector end of the cable, consider using a lightning arrester immediately before the cable enters the building

Grounding

It is important that the wireless bridge, cables, and any supporting structures are properly grounded. The wireless bridge unit includes a grounding screw for attaching a ground wire. Be sure that grounding is available and that it meets local and national electrical codes.

Chapter 4

Hardware Installation

Before mounting antennas to set up your wireless bridge links, be sure you have selected appropriate locations for each antenna. Follow the guidance and information in Chapter 2, “Wireless Link Planning.”

Also, before mounting units in their intended locations, you should first perform initial configuration and test the basic operation of the wireless bridge links in a controlled environment over a very short range. (See the section “Testing Basic Link Operation” in this chapter.)

The wireless bridge includes its own bracket kit for mounting the unit to a 1.5 to 2 inch diameter steel pole or tube. The pole-mounting bracket allows the unit to be mounted to part of a radio mast or tower structure. The unit also has a wall-mounting bracket kit that enables it to be fixed to a building wall or roof when using external antennas.

Hardware installation of the wireless bridge involves these steps:

1. Mount the unit on a wall, pole, mast, or tower using the mounting bracket.
2. Mount external antennas on the same supporting structure as the bridge and connect them to the bridge unit.
3. Connect the Ethernet cable and a grounding wire to the unit.
4. Connect the power injector to the Ethernet cable, a local LAN switch, and an AC power source.

5. Align antennas at both ends of the link.

Testing Basic Link Operation

Set up the units over a very short range (15 to 25 feet), either outdoors or indoors. Connect the units as indicated in this chapter and be sure to perform all the basic configuration tasks outlined above. When you are satisfied that the links are operating correctly, proceed to mount the units in their intended locations.

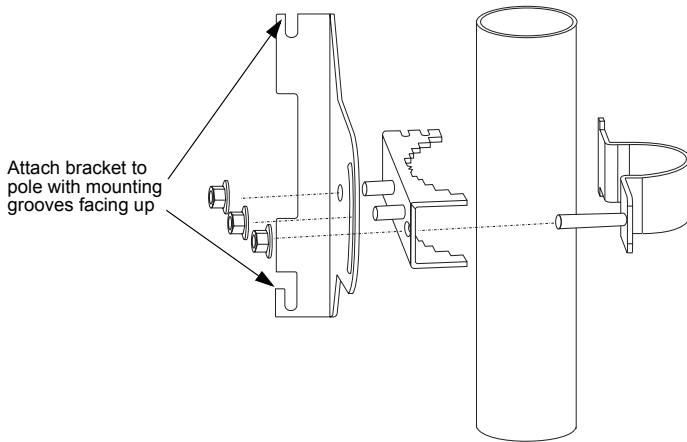
Mount the Unit

Using the Pole-Mounting Bracket

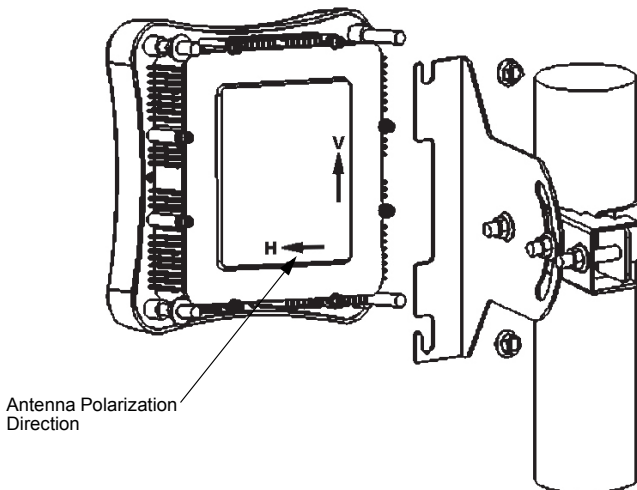
Perform the following steps to mount the unit to a 1.5 to 2 inch diameter steel pole or tube using the mounting bracket:

1. Always attach the bracket to a pole with the open end of the mounting grooves facing up.
2. Place the U-shaped part of the bracket around the pole and tighten the securing nut just enough to hold the bracket to the pole. (The bracket may need to be rotated around the pole during the alignment process.)

Mount the Unit



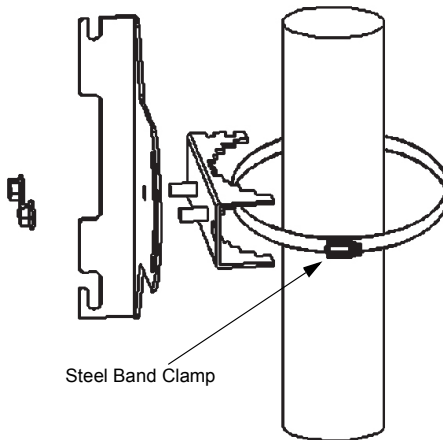
3. Use the included nuts to tightly secure the wireless bridge to the bracket. Be sure to take account of the antenna polarization direction; both antennas in a link must be mounted with the same polarization.



Hardware Installation

Mounting on Larger Diameter Poles

In addition, there is a method for attaching the pole-mounting bracket to a pole that is 2 to 5 inches in diameter using an adjustable steel band clamp (not included in the kit). A steel band clamp up to 0.5 inch (1.27 cm) wide can be threaded through the main part of the bracket to secure it to a larger diameter pole without using the U-shaped part of the bracket. This method is illustrated in the following figure.



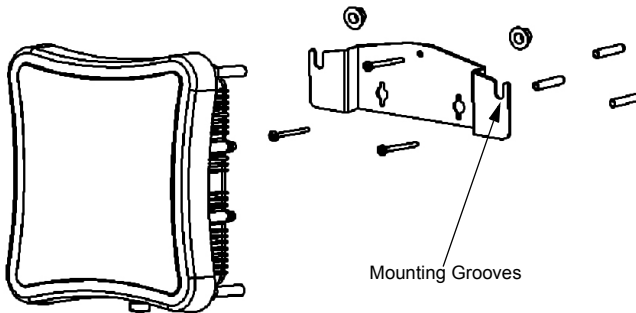
Using the Wall-Mounting Bracket

Perform the following steps to mount the unit to a wall using the wall-mounting bracket:

Note: The wall-mounting bracket does not allow the wireless bridge's integrated antenna to be aligned. It is intended for use with the unit using an external antenna.

1. Always attach the bracket to a wall with the open end of the mounting grooves facing up (see following figure).

Connect External Antennas



2. Position the bracket in the intended location and mark the position of the three mounting screw holes.
3. Drill three holes in the wall that match the screws and wall plugs included in the bracket kit, then secure the bracket to the wall.
4. Use the included nuts to tightly secure the wireless bridge to the bracket.

Connect External Antennas

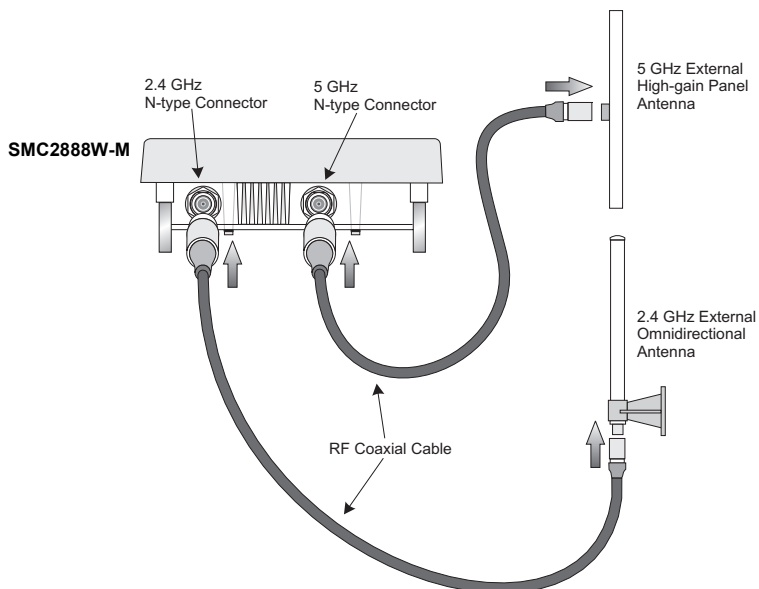
When deploying a SMC2888W-M Master bridge unit for a bridge link or access point operation, you need to mount external antennas and connect them to the bridge. Typically, a bridge link requires a 5 GHz antenna, and access point operation a 2.4 GHz antenna. SMC2888W-S Slave units also require an external antenna for 2.4 GHz operation.

Perform these steps:

1. Mount the external antenna to the same supporting structure as the bridge, within 3 m (10 ft) distance, using the bracket supplied in the antenna package.

Hardware Installation

2. Connect the antenna to the bridge's N-type connector.
3. Apply weatherproofing tape to the antenna connectors to help prevent water entering the connectors.



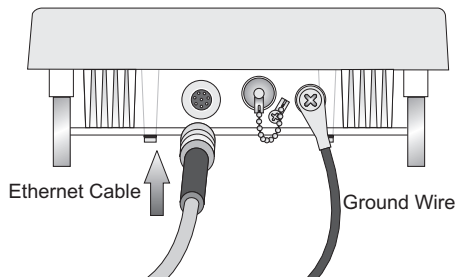
Connect Cables to the Unit

1. Attach the Ethernet cable to the Ethernet port on the wireless bridge.

Note: The Ethernet cable included with the package is 30 m (100 ft) long. To wire a longer cable (maximum 100 m, 325 ft), use the connector pinout information in Appendix B.

2. For extra protection against rain or moisture, apply weatherproofing tape (not included) around the Ethernet connector.
3. Be sure to ground the unit with an appropriate grounding wire (not included) by attaching it to the grounding screw on the unit.

Caution: Be sure that grounding is available and that it meets local and national electrical codes. For additional lightning protection, use lightning rods, lightning arrestors, or surge suppressors.



Connect the Power Injector

To connect the wireless bridge to a power source:

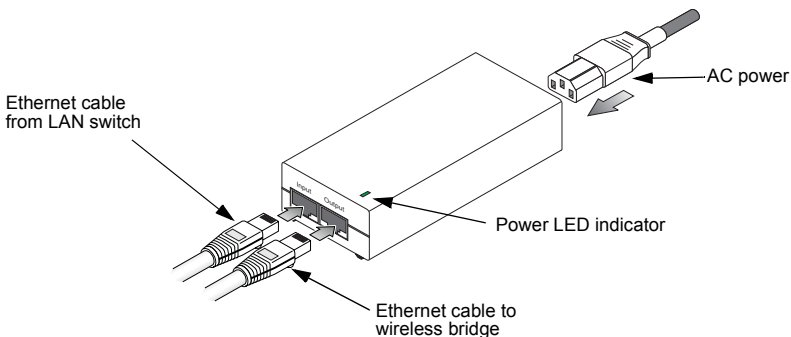
Caution: Do not install the power injector outdoors. The unit is for indoor installation only.

Hardware Installation

Note: The wireless bridge's Ethernet port does not support Power over Ethernet (PoE) based on the IEEE 802.3af standard. Do not try to power the unit by connecting it directly to a network switch that provides IEEE 802.3af PoE. Always connect the unit to the included power injector module.

1. Connect the Ethernet cable from the wireless bridge to the RJ-45 port labeled "Output" on the power injector.
2. Connect a straight-through unshielded twisted-pair (UTP) cable from a local LAN switch to the RJ-45 port labeled "Input" on the power injector. Use Category 5 or better UTP cable for 10/100BASE-TX connections.

Note: The RJ-45 port on the power injector is an MDI port. If connecting directly to a computer for testing the link, use a crossover cable.



3. Insert the power cable plug directly into the standard AC receptacle on the power injector.
4. Plug the other end of the power cable into a grounded, 3-pin socket, AC power source.

Note: For International use, you may need to change the AC line cord. You must use a line cord set that has been approved for the receptacle type in your country.

5. Check the LED on top of the power injector to be sure that power is being supplied to the wireless bridge through the Ethernet connection.

Align Antennas

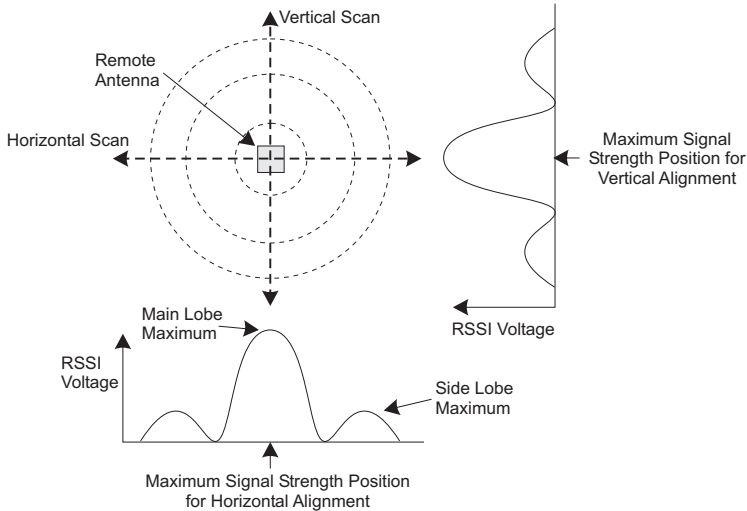
After wireless bridge units have been mounted, connected, and their radios are operating, the antennas must be accurately aligned to ensure optimum performance on the bridge links. This alignment process is particularly important for long-range point-to-point links. In a point-to-multipoint configuration the Master bridge uses an omnidirectional or sector antenna, which does not require alignment, but Slave bridges still need to be correctly aligned with the Master bridge antenna.

- **Point-to-Point Configurations** – In a point-to-point configuration, the alignment process requires two people at each end of the link. The use of cell phones or two-way radio communication may help with coordination. To start, you can just point the antennas at each other, using binoculars or a compass to set the general direction. For accurate alignment, you must connect a DC voltmeter to the RSSI connector on the wireless bridge and monitor the voltage as the antenna moves horizontally and vertically.
- **Point-to-Multipoint Configurations** – In a point-to-multipoint configuration all Slave bridges must be aligned with the Master bridge antenna. The alignment process is the same as in point-to-point links, but only the Slave end of the link requires the alignment.

The RSSI connector provides an output voltage between 0 and 3.28 VDC that is proportional to the received radio signal strength. The higher the voltage reading, the stronger the signal. The radio signal from the remote antenna can be seen to have a

Hardware Installation

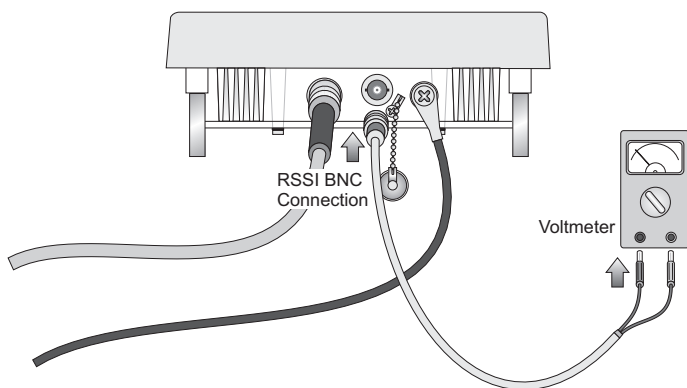
strong central main lobe and smaller side lobes. The object of the alignment process is to set the antenna so that it is receiving the strongest signal from the central main lobe.



To align the antennas in the link using the RSSI output voltage, start with one antenna fixed and then perform the following procedure on the other antenna:

Note: The RSSI output can be configured through management interfaces to output a value for specific WDS ports. See page 6-54 for more information.

1. Remove the RSSI connector cover and connect a voltmeter using a cable with a male BNC connector (not included).



2. Pan the antenna horizontally back and forth while checking the RSSI voltage. If using the pole-mounting bracket with the unit, you must rotate the mounting bracket around the pole. Other external antenna brackets may require a different horizontal adjustment.
3. Find the point where the signal is strongest (highest voltage) and secure the horizontal adjustment in that position.

Note: Sometimes there may not be a central lobe peak in the voltage because vertical alignment is too far off; only two similar peaks for the side lobes are detected. In this case, fix the antenna so that it is halfway between the two peaks.

4. Loosen the vertical adjustment on the mounting bracket and tilt the antenna slowly up and down while checking the RSSI voltage.
5. Find the point where the signal is strongest and secure the vertical adjustment in that position.
6. Remove the voltmeter cable and replace the RSSI connector cover.

Chapter 5

Initial Configuration

The wireless bridge offers a variety of management options, including a web-based interface, a command line interface (CLI), or using SNMP management software.

Most initial configuration steps can be made through the web browser interface using the Setup Wizard (page 5-4). However, for units that do not have a preset country code, you must first set the country code using the CLI.

Note: Units sold in some countries are not configured with a specific country code. You must use the CLI to set the country code and enable wireless operation (page 5-2).

The wireless bridge requests an IP address via DHCP by default. If no response is received from a DHCP server, then the wireless bridge uses the default address 192.168.2.2. If this address is not compatible with your network, you can first perform initial configuration using a PC that has IP settings compatible with this subnet (for example, 192.168.2.3) and connecting it directly to the wireless bridge. When the basic configuration is completed, you can set new IP settings for the wireless bridge before connecting it to your network.

Initial Setup through the CLI

The wireless bridge provides access to the CLI through a Telnet connection. You can open a Telnet session by performing these steps:

1. From the host computer, enter the Telnet command and the IP address of the wireless bridge unit (default 192.168.2.2 if not set via DHCP).
2. At the prompt, enter “admin” for the user name.
3. The default password is “smcadmin”.

The CLI will display the “Dual Outdoor#” prompt to show that you are using executive access mode (i.e., Exec).

```
Username: admin
Password:
Dual Outdoor#
```

For a full description of how to use the CLI, see “Using the Command Line Interface” on page 7-1. For a list of all the CLI commands and detailed information on using the CLI, refer to “Command Groups” on page 7-9.

Initial Configuration Steps

Setting the Country Code – Regulations for wireless products differ from country to country. Setting the country code restricts the wireless bridge to use only the radio channels and power settings permitted in the specified country of operation. If the wireless bridge unit is shipped with a preset country code, you are not permitted to change it, as required by country regulations. If the unit is set to the default “99,” you must set the country code to the country of operation.

Initial Setup through the CLI

At the Exec prompt, type “country ?” to display the list of country codes. Check the code for your country, then enter the country command again followed by your country code (e.g., IE for Ireland).

```
Dual Outdoor#country ie
Dual Outdoor#
```

Setting the IP Address – By default, the wireless bridge is configured to obtain IP address settings from a DHCP server. You may also use the CLI to assign an IP address that is compatible with your network.

Type “configure” to enter configuration mode, then type “interface ethernet” to access the Ethernet interface-configuration mode.

```
Dual Outdoor#configure
Dual Outdoor(config)#interface ethernet
Dual Outdoor(config-if)#
```

First type “no ip dhcp” to disable DHCP client mode. Then type “ip address *ip-address netmask gateway*,” where “ip-address” is the wireless bridge’s IP address, “netmask” is the network mask for the network, and “gateway” is the default gateway router. Check with your system administrator to obtain an IP address that is compatible with your network.

```
Dual Outdoor(if-ethernet)#no ip dhcp
Dual Outdoor(if-ethernet)#ip address 192.168.2.2 255.255.255.0
192.168.2.254
Dual Outdoor(if-ethernet)#
```

Initial Configuration

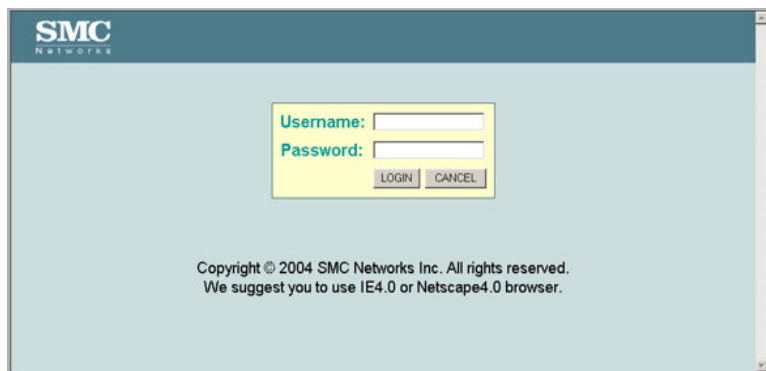
After configuring the wireless bridge's IP parameters, you can access the management interface from anywhere within the attached network. The command line interface can also be accessed using Telnet from any computer attached to the network.

Using the Web-based Management Setup Wizard

There are only a few basic steps you need to complete to set up the wireless bridge for your network. The Setup Wizard takes you through configuration procedures for the radio channel selection, IP configuration, and basic WEP encryption for wireless security.

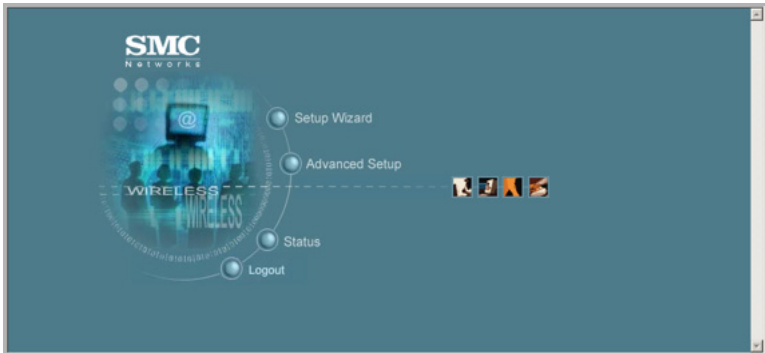
The wireless bridge can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above). Enter the IP configured for the unit or the default IP address: <http://192.168.2.2>

Logging In – Enter the default username “admin” and password “smcadmin” click LOGIN. For information on configuring a user name and password, refer to page 6-33.

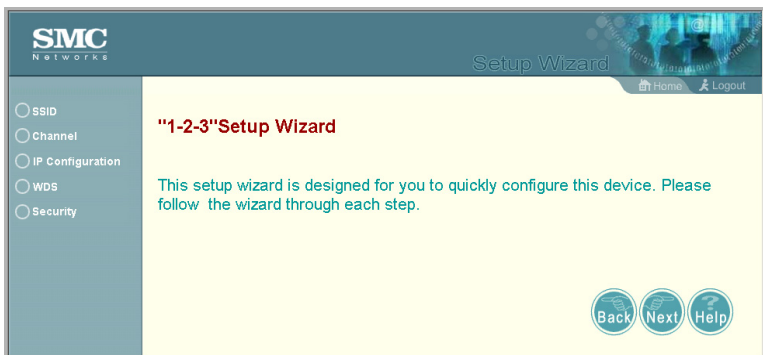


Using the Web-based Management Setup Wizard

The home page displays the Main Menu.



Launching the Setup Wizard – To perform initial configuration, click Setup Wizard on the home page, then click on the [Next] button to start the process.



- 1. Service Set ID** – Enter the service set identifier in the SSID box which all wireless 802.11g clients must use to associate with the access point. The SSID is case sensitive and can consist of up to 32 alphanumeric characters (Default: SMC).

Initial Configuration

The screenshot shows the 'Setup Wizard' interface for SMC Networks. On the left, a sidebar lists configuration steps: SSID (checked), Channel, IP Configuration, WDS, and Security. The main content area is titled 'SSID' and explains that the SSID is used for radio identification. It includes a text input field for the SSID, which contains the value 'SMC'. At the bottom right, there are three circular buttons labeled 'Back', 'Next', and 'Help'.

- 2. Radio Channel** – You must enable radio communications for the 802.11a and 802.11g radios and set the operating channel.

The screenshot shows the 'Setup Wizard' interface for SMC Networks, specifically the 'Channel' configuration page. The sidebar on the left shows 'Channel' as the current step, with 'SSID' also checked. The main content area is titled 'Channel' and provides instructions on enabling radio channels. It includes sections for '802.11a' and '802.11g', each with an 'Enable' checkbox. Below these, it states that there are no 11a or 11g channels supported by the current country. At the bottom, there is a radio button selection for 'Auto Channel Select', with 'Disable' selected and 'Enable' as an alternative. At the bottom right, there are three circular buttons labeled 'Back', 'Next', and 'Help'.

- 802.11a

Using the Web-based Management Setup Wizard

Turbo Mode – If you select Enable, the wireless bridge will operate in turbo mode with a data rate of up to 108 Mbps. Normal mode supports 13 channels, Turbo mode supports only 5 channels. (Default: Disable)

802.11a Radio Channel – Set the operating radio channel number. (Default: 56ch, 5.280 GHz)

Auto Channel Select – Select Enable to automatically select an unoccupied radio channel. (Default: Enable)

- 802.11b/g

802.11g Radio Channel: Set the operating radio channel number. (Range 1-11; Default: 1)

Initial Configuration

Note: Available channel settings are limited by local regulations which determine which channels are available.

- 3. IP Configuration** – Either enable or disable (Dynamic Host Configuration Protocol (DHCP) for automatic IP configuration. If you disable DHCP, then manually enter the IP address and subnet mask. If a management station exists on another network segment, then you must enter the IP address for a gateway that can route traffic between these segments. Then enter the IP address for the primary and secondary Domain Name Servers (DNS) servers to be used for host-name to IP address resolution.

The screenshot shows the SMC Networks Setup Wizard interface. On the left is a sidebar with navigation options: SSID (checked), Channel (checked), IP Configuration (checked), WDS (unchecked), and Security (unchecked). The main content area is titled 'TCP / IP Settings' and contains a 'DHCP Client' section. Under 'DHCP Client', the 'Enable' radio button is selected, with the text 'The Access Point will obtain the IP Address from the DHCP Server'. Below this, there are five input fields: 'IPAddress' (192.168.2.2), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (0.0.0.0), 'Primary DNS Address' (0.0.0.0), and 'Secondary DNS Address' (0.0.0.0). At the bottom right of the main area are three circular buttons: 'Back', 'Next', and 'Help'.

- **DHCP Client** – With DHCP Client enabled, the IP address, subnet mask and default gateway can be dynamically assigned to the access point by the network DHCP server. (Default: Enable)

Note: If there is no DHCP server on your network, then the access point will automatically start up with its default IP address, 192.168.2.2.

Using the Web-based Management Setup Wizard

4. **WDS** – To set up a wireless bridge link, you must configure the WDS forwarding table by specifying the Ethernet MAC address of the bridge to which you want to forward traffic. For a Slave bridge unit, you need to specify the MAC address of the wireless bridge unit at the opposite end of the link. For a Master bridge unit, you need to specify the MAC addresses of all the Slave bridge units in the network.

The screenshot shows the SMC Networks Setup Wizard interface. On the left is a sidebar with navigation links: SSID, Channel, IP Configuration, WDS (selected), and Security. The main content area is titled 'WDS Settings' and 'Slave Mode'. It contains several configuration fields: 'MAC address' with a text input showing '0F:00:22:44:99:0F'; 'Port status' with radio buttons for 'Disable' and 'Enable' (selected); 'Channel Scan' with radio buttons for 'Disable' and 'Enable' (selected); 'Mode' with radio buttons for 'Normal' and 'Turbo' (selected); and 'Distance' with a text input showing '00' followed by 'KM'. At the bottom right are three circular buttons: 'Back', 'Next', and 'Help'. The top right of the interface includes 'Home' and 'Logout' links.

WDS Settings	
Slave Mode	
MAC address	<input type="text" value="0F:00:22:44:99:0F"/>
Port status	<input checked="" type="radio"/> Disable <input checked="" type="radio"/> Enable
Channel Scan	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Mode	<input checked="" type="radio"/> Normal <input type="radio"/> Turbo
Distance	<input type="text" value="00"/> KM

Back Next Help

5. **Security** (802.11g) – Set the Authentication Type to “Open System” to allow open access without authentication, or “Shared Key” to require authentication based on a shared key. Enable Wired Equivalent Privacy (WEP) to encrypt data transmissions. To configure other security features use the Advanced Setup menu as described in Chapter 5.

The screenshot shows the SMC Network Setup Wizard, specifically the Security configuration page. The left sidebar lists the setup steps: SSID, Channel, IP Configuration, WDS, and Security (which is currently selected). The main content area is titled 'Security' and contains three sections: 'Authentication Type Setup' with radio buttons for 'Open System' (selected) and 'Shared Key'; 'Wired Equivalent Privacy (WEP) Setup' with radio buttons for 'Disable' (selected) and 'Enable'; and 'Shared Key Setup' with radio buttons for '64 Bit', '128 Bit', and '152 Bit'. Below these, the 'Key Type' section has radio buttons for 'Hexadecimal' (selected) and 'Alphanumeric'. Instructions specify the number of characters to enter for each key type and bit length combination. At the bottom, there is a table for entering keys:

Key Number	Key
Key 1	<input type="text"/>

At the bottom right of the wizard are three buttons: 'Back', 'Finish', and 'Help'.

Authentication Type – Use “Open System” to allow open access to all wireless clients without performing authentication, or “Shared Key” to perform authentication based on a shared key that has been distributed to all stations. (Default: Open System)

WEP – Wired Equivalent Privacy is used to encrypt transmissions passing between wireless clients and the access point. (Default: Disabled)

Shared Key Setup – If you select “Shared Key” authentication type or enable WEP, then you also need to configure the shared key by selecting 64-bit or 128-bit key type, and entering a

Using the Web-based Management Setup Wizard

hexadecimal or ASCII string of the appropriate length. The key can be entered as alphanumeric characters or hexadecimal (0~9, A~F, e.g., D7 0A 9C 7F E5). (Default: 128 bit, hexadecimal key type)

64-Bit Manual Entry: The key can contain 10 hexadecimal digits, or 5 alphanumeric characters.

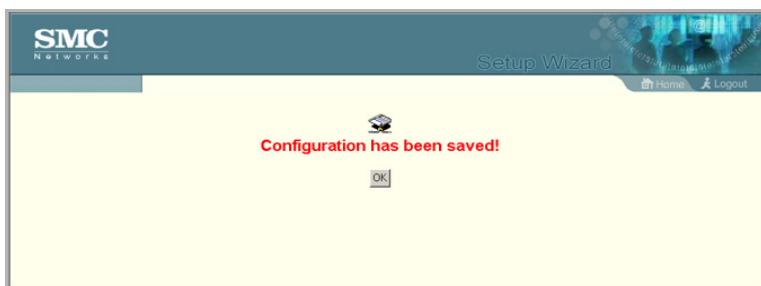
128-Bit Manual Entry: The key can contain 26 hexadecimal digits or 13 alphanumeric characters.

152-Bit Manual Entry: The key can contain 32 hexadecimal digits or 16 alphanumeric characters.

Note: All wireless devices must be configured with the same Key ID values to communicate with the access point.

6. Click Finish.

7. Click the OK button to restart the access point.



Initial Configuration

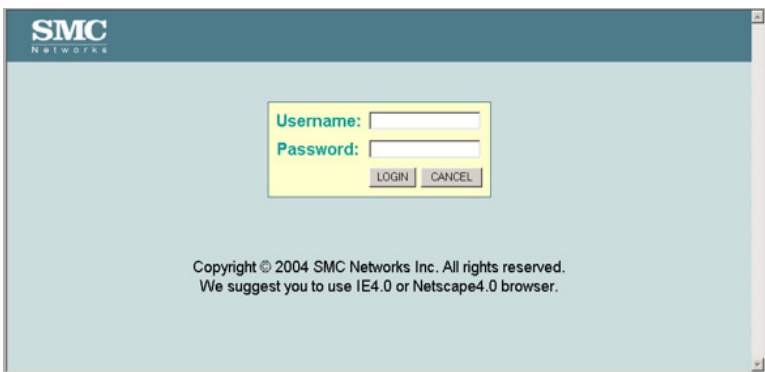
Chapter 6

System Configuration

Before continuing with advanced configuration, first complete the initial configuration steps described in Chapter 5 to set up an IP address for the wireless bridge.

The wireless bridge can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above). Enter the default IP address: `http://192.168.2.2`

To log into the wireless bridge, enter the default user name “admin” and password “smcadmin” then click LOGIN.



The image shows a web browser window displaying the SMC Networks login page. The page has a light blue background. At the top left, the SMC Networks logo is visible. In the center, there is a yellow rectangular box containing the login fields. The 'Username:' label is in blue, followed by a text input field. The 'Password:' label is also in blue, followed by a text input field. Below the password field are two buttons: 'LOGIN' and 'CANCEL'. At the bottom of the page, there is a copyright notice: 'Copyright © 2004 SMC Networks Inc. All rights reserved. We suggest you to use IE4.0 or Netscape4.0 browser.'

SMC
NETWORKS

Username:

Password:

LOGIN CANCEL

Copyright © 2004 SMC Networks Inc. All rights reserved.
We suggest you to use IE4.0 or Netscape4.0 browser.

System Configuration

When the home page displays, click on Advanced Setup. The following page will display.



The information in this chapter is organized to reflect the structure of the web screens for easy reference. However, it is recommended that you configure a user name and password as the first step under advanced configuration to control management access to the wireless bridge (page 6-33).

Advanced Configuration

The Advanced Configuration pages include the following options.

Menu	Description	Page
System	Configures basic administrative and client access	6-4
Identification	Specifies the system name, location and contact information	6-4
TCP / IP Settings	Configures the IP address, subnet mask, gateway, and domain name servers	6-7
Radius	Configures the RADIUS server for wireless client authentication	6-10
PPPoE Settings	Configures PPPoE on the Ethernet interface for a connection to an ISP	6-13
Authentication	Configures 802.1X client authentication and MAC address authentication	6-16
Filter Control	Enables VLAN support and filters traffic matching specific Ethernet protocol types	6-26
SNMP	Controls access to this wireless bridge from management stations using SNMP, as well as the hosts that will receive trap messages	6-30
Administration	Configures user name and password for management access; upgrades software from local file, FTP or TFTP server; resets configuration settings to factory defaults; and resets the wireless bridge	6-33
System Log	Controls logging of error messages; sets the system clock via SNTP server or manual configuration	6-38
WDS	Sets the MAC addresses of other units in the wireless bridge network	6-43
Bridge	Sets the time for aging out entries in the bridge MAC address table	6-45
STP	Configures Spanning Tree Protocol parameters	6-47

System Configuration

Menu	Description	Page
RSSI	Controls the maximum RSSI voltage output for specific WDS ports	6-54
Radio Interface A	Configures the IEEE 802.11a interface	6-56
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, and beacon settings	6-57
Security	Configures data encryption using Wired Equivalent Protection (WEP) or Wi-Fi Protected Access (WPA)	6-66
Radio Interface G	Configures the IEEE 802.11b/g interface	6-63
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, and beacon settings	6-63
Security	Configures data encryption using Wired Equivalent Protection (WEP) or Wi-Fi Protected Access (WPA)	6-66

System Identification

The system information parameters for the wireless bridge can be left at their default settings. However, modifying these parameters can help you to more easily distinguish different devices in your network.

The wireless bridge allows the selection of the band to be used for bridge links. The bridge band can support no wireless clients. Alternatively, bridging can be disabled and both bands can support access point functions.

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a sidebar menu under the 'SYSTEM' heading, listing various configuration options like Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, Administration, System Log, WDS, Bridge, STP, and RSSI. The main content area is titled 'Identification' and contains three sections: 'System Name' with a text input field containing 'MRW55 Wireless Outdoor Bridge/AP' and an explanatory note; 'Outdoor Bridge Band' with radio buttons for 'A', 'G', and 'None', and an explanatory note; and 'Location' and 'Contact' with empty text input fields. At the bottom right are 'Apply', 'Cancel', and 'Help' buttons.

System Name – An alias for the wireless bridge, enabling the device to be uniquely identified on the network. (Default: Dual Band Outdoor AP; Range: 1-22 characters)

Outdoor Bridge Band – Selects the radio band used for bridge links.

- A – Bridging is supported on the 802.11a 5 GHz band.
- G – Bridging is supported on the 802.11b/g 2.4 GHz band.
- None – Bridging is not supported on either radio band. Allows both bands to support access point operations for wireless clients.

Location – A text string that describes the system location. (Maximum length: 20 characters)

Contact – A text string that describes the system contact. (Maximum length: 255 characters)

System Configuration

CLI Commands for System Identification – Enter the global configuration mode and use the **system name** command to specify a new system name. Use the **snmp-server location** and **snmp-server contact** commands to indicate the physical location of the wireless bridge and define a system contact. Then return to the Exec mode, and use the **show system** command to display the changes to the system identification settings.

```
AP#configure 7-10
AP(config)#system name R&D 7-19
AP(config)#snmp-server location building-1 7-38
AP(config)#snmp-server contact Paul 7-35
AP(config)#exit
AP#show system 7-22

System Information
=====
Serial Number      : 0000000005
System Up time     : 0 days, 0 hours, 35 minutes, 56 seconds
System Name        : R&D
System Location    : building-1
System Contact     : Paul
System Country Code : US - UNITED STATES
MAC Address        : 00-30-F1-BE-F4-96
IP Address         : 192.168.2.2
Subnet Mask        : 255.255.255.0
Default Gateway    : 0.0.0.0
VLAN State         : DISABLED
Native VLAN ID     : 1
IAPP State         : ENABLED
DHCP Client        : ENABLED
HTTP Server        : ENABLED
HTTP Server Port   : 80
Slot Status        : Dual band(a/g)
Software Version    : v1.1.0.3
=====

AP#
```

CLI Commands for Bridge Band Selection – Enter the global configuration mode and use the **wds channel** command to specify the bridge band.

```
AP#configure 7-10
AP(config)#wds channel a 7-62
AP(config)#
```

TCP / IP Settings

Configuring the wireless bridge with an IP address expands your ability to manage the wireless bridge. A number of wireless bridge features depend on IP addressing to operate.

Note: You can use the web browser interface to access IP addressing only if the wireless bridge already has an IP address that is reachable through your network.

By default, the wireless bridge will be automatically configured with IP settings from a Dynamic Host Configuration Protocol (DHCP) server. However, if you are not using a DHCP server to configure IP addressing, use the CLI to manually configure the initial IP values (page 5-2). After you have network access to the wireless bridge, you can use the web browser interface to modify the initial IP configuration, if needed.

Note: If there is no DHCP server on your network, or DHCP fails, the wireless bridge will automatically start up with a default IP address of 192.168.2.2.

System Configuration

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM (containing Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, Administration, System Log, WDS, Bridge, STP, and RSSI), RADIO INTERFACE A (containing Radio Settings and Security), and RADIO INTERFACE G (containing Radio Settings and Security). The main content area is titled 'TCP / IP Settings' and contains a 'DHCP Client' section. Two radio buttons are present: 'Enable' (selected) and 'Disable'. Below these are five input fields: IP Address (192.168.2.2), Subnet Mask (255.255.255.0), Default Gateway (0.0.0.0), Primary DNS Address (0.0.0.0), and Secondary DNS Address (0.0.0.0). At the bottom right are three buttons: Apply, Cancel, and Help.

DHCP Client	
<input type="radio"/> Enable	The Access Point will obtain the IP Address from the DHCP Server
<input checked="" type="radio"/> Disable	The Access Point will use the following IP Setup
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0

DHCP Client (Enable) – Select this option to obtain the IP settings for the wireless bridge from a DHCP (Dynamic Host Configuration Protocol) server. The IP address, subnet mask, default gateway, and Domain Name Server (DNS) address are dynamically assigned to the wireless bridge by the network DHCP server.
(Default: Enabled)

DHCP Client (Disable) – Select this option to manually configure a static address for the wireless bridge.

- **IP Address:** The IP address of the wireless bridge. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets.

- **Default Gateway:** The default gateway is the IP address of the router for the wireless bridge, which is used if the requested destination address is not on the local subnet.
- If you have management stations, DNS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided. Otherwise, leave the address as all zeros (0.0.0.0).
- **Primary and Secondary DNS Address:** The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.
- If you have one or more DNS servers located on the local network, type the IP addresses in the text fields provided. Otherwise, leave the addresses as all zeros (0.0.0.0).

CLI Commands for TCP/IP Settings – From the global configuration mode, enter the interface configuration mode with the interface ethernet command. Use the **ip dhcp** command to enable the DHCP client, or **no ip dhcp** to disable it. To manually configure an address, specify the new IP address, subnet mask, and default gateway using the **ip address** command. To specify DNS server addresses use the **dns server** command. Then use the **show interface ethernet** command from the Exec mode to display the current IP settings.

System Configuration

AP(config)#interface ethernet	7-91
Enter Ethernet configuration commands, one per line.	
AP(if-ethernet)#no ip dhcp	7-94
AP(if-ethernet)#ip address 192.168.1.2	
255.255.255.0 192.168.1.253	7-93
AP(if-ethernet)#dns primary-server 192.168.1.55	7-92
AP(if-ethernet)#dns secondary-server 10.1.0.55	7-92
AP(config)#end	7-11
AP#show interface ethernet	7-96
Ethernet Interface Information	
=====	
IP Address : 192.168.1.2	
Subnet Mask : 255.255.255.0	
Default Gateway : 192.168.1.253	
Primary DNS : 192.168.1.55	
Secondary DNS : 10.1.0.55	
Admin status : Up	
Operational status : Up	
=====	
AP#	

Radius

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network.

A primary RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible.

Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

The screenshot displays the SMC Network Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM (including Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, Administration, System Log, WDS, Bridge, STP, and RSSI), RADIO INTERFACE A (Radio Settings, Security), and RADIO INTERFACE G (Radio Settings, Security). The main content area is titled 'Radius' and contains two sections: 'Primary Radius Server Setup' and 'Secondary Radius Server Setup'. Each section has five input fields: IP Address (0.0.0.0), Port (1812), Key (empty), Timeout (seconds) (5), and Retransmit attempts (3). At the bottom right of the main area are three buttons: Apply, Cancel, and Help.

Primary Radius Server Setup	
IP Address	0.0.0.0
Port	1812
Key	
Timeout (seconds)	5
Retransmit attempts	3

Secondary Radius Server Setup	
IP Address	0.0.0.0
Port	1812
Key	
Timeout (seconds)	5
Retransmit attempts	3

Primary Radius Server Setup – Configure the following settings to use RADIUS authentication on the access point.

- **IP Address:** Specifies the IP address or host name of the RADIUS server.
- **Port:** The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

System Configuration

- **Key:** A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- **Timeout:** Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 5)
- **Retransmit attempts:** The number of times the access point tries to resend a request to the RADIUS server before authentication fails. (Range: 1-30; Default: 3)

Note: For the Timeout and Retransmit attempts fields, accept the default values unless you experience problems connecting to the RADIUS server over the network.

Secondary Radius Server Setup – Configure a secondary RADIUS server to provide a backup in case the primary server fails. The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodically attempts to establish communication again with primary server. If communication with the primary server is re-established, the secondary server reverts to a backup role.

CLI Commands for RADIUS – From the global configuration mode, use the **radius-server address** command to specify the address of the primary or secondary RADIUS servers. (The following example configures the settings for the primary RADIUS server.) Configure the other parameters for the RADIUS server. Then use the **show show radius** command from the Exec mode

to display the current settings for the primary and secondary RADIUS servers.

```
AP(config)#radius-server address 192.168.1.25          7-45
AP(config)#radius-server port 181                      7-46
AP(config)#radius-server key green                    7-47
AP(config)#radius-server timeout 10                   7-48
AP(config)#radius-server retransmit 5                 7-47
AP(config)#exit
AP#show radius                                         7-48

Radius Server Information
=====
IP                : 192.168.1.25
Port              : 181
Key               : *****
Retransmit        : 5
Timeout           : 10
=====

Radius Secondary Server Information
=====
IP                : 0.0.0.0
Port              : 1812
Key               : *****
Retransmit        : 3
Timeout           : 5
=====
AP#
```

PPPoE Settings

The wireless bridge uses a Point-to-Point Protocol over Ethernet (PPPoE) connection, or tunnel, only for management traffic between the wireless bridge and a remote PPPoE server (typically at an ISP). Examples of management traffic that may be initiated by the wireless bridge and carried over a PPPoE tunnel are RADIUS, Syslog, or DHCP traffic.

System Configuration

The screenshot displays the SMC Networks Advanced Setup web interface. On the left is a navigation menu with categories: SYSTEM, RADIO INTERFACE A, and RADIO INTERFACE G. The SYSTEM category is expanded, showing options like Identification, TCP/IP Settings, Radius, PPPoE Settings (highlighted), Authentication, Filter Control, SNMP, Administration, System Log, WDS, Bridge, STP, and RSSI. The main content area is titled 'PPPoE Settings' and contains several configuration fields: 'PPP over Ethernet' with radio buttons for 'Disable' (selected) and 'Enable'; 'PPPoE Username' and 'PPPoE Password' with text input fields; 'Confirm Password' with a text input field; 'PPPoE Service Name' with a text input field; and 'IP Allocation Mode' with radio buttons for 'Automatically allocated' (selected) and 'Static assigned'. At the bottom right of the main area are three circular buttons: 'Apply', 'Cancel', and 'Help'.

PPPoE Settings	
PPP over Ethernet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
PPPoE Username	<input type="text"/>
PPPoE Password	<input type="text"/>
Confirm Password	<input type="text"/>
PPPoE Service Name	<input type="text"/>
IP Allocation Mode	<input checked="" type="radio"/> Automatically allocated <input type="radio"/> Static assigned

PPP over Ethernet – Enable PPPoE on the RJ-45 Ethernet interface to pass management traffic between the unit and a remote PPPoE server. (Default: Disable)

PPPoE Username – The user name assigned for the PPPoE tunnel. (Range: 1-63 alphanumeric characters)

PPPoE Password – The password assigned for the PPPoE tunnel. (Range: 1-63 alphanumeric characters)

Confirm Password – Use this field to confirm the PPPoE password.

PPPoE Service Name – The service name assigned for the PPPoE tunnel. The service name is normally optional, but may be required by some service providers. (Range: 1-63 alphanumeric characters)

IP Allocation Mode – This field specifies how IP addresses for the PPPoE tunnel are configured on the RJ-45 interface. The allocation mode depends on the type of service provided by the PPPoE server. If automatic mode is selected, DHCP is used to allocate the IP addresses for the PPPoE connection. If static addresses have been assigned to you by the service provider, you must manually enter the assigned addresses. (Default: Automatic)

- Automatically allocated: IP addresses are dynamically assigned by the service provider during PPPoE session initialization.
- Static assigned: Fixed addresses are assigned by the service provider for both the local and remote IP addresses.

Local IP Address – IP address of the local end of the PPPoE tunnel. (Must be entered for static IP allocation mode.)

Remote IP Address – IP address of the remote end of the PPPoE tunnel. (Must be entered for static IP allocation mode.)

CLI Commands for PPPoE – From the CLI configuration mode, use the **interface ethernet** command to access interface configuration mode. Use the **ip pppoe** command to enable PPPoE on the Ethernet interface. Use the other PPPoE commands shown in the example below to set a user name and password, IP settings, and other PPPoE parameters as required by the service provider. The **pppoe restart** command can then be used to start a new connection using the modified settings. To display the current PPPoE settings, use the **show pppoe** command from the Exec mode.

System Configuration

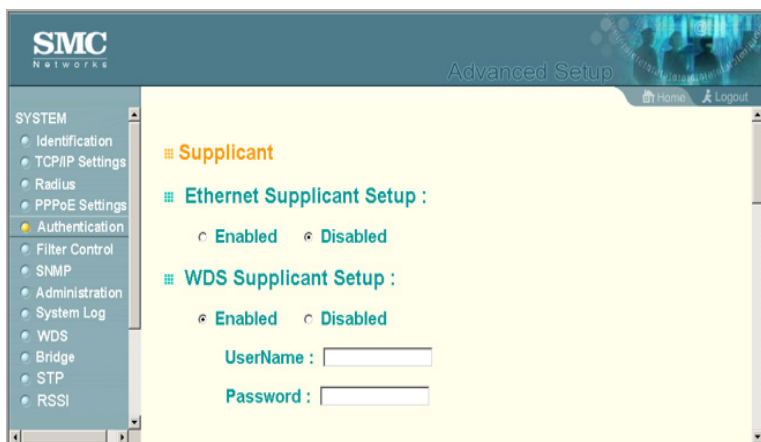
```
AP(config)#interface ethernet                                7-91
Enter Ethernet configuration commands, one per line.
AP(if-ethernet)#ip pppoe                                    7-81
AP(if-ethernet)#pppoe username mike                        7-87
AP(if-ethernet)#pppoe password 12345                       7-88
AP(if-ethernet)#pppoe service-name classA                  7-89
AP(if-ethernet)#pppoe ip allocation mode static             7-82
AP(if-ethernet)#pppoe local ip 10.7.1.200                  7-86
AP(if-ethernet)#pppoe remote ip 192.168.1.20               7-86
AP(if-ethernet)#pppoe ipcp dns                             7-83
AP(if-ethernet)#pppoe lcp echo-interval 30                 7-84
AP(if-ethernet)#pppoe lcp echo-failure 5                   7-85
AP(if-ethernet)#pppoe restart                               7-89
AP(if-ethernet)#end
AP#show pppoe                                              7-90

PPPoE Information
=====
State                : Link up
Username             : mike
Service Name         : classA
IP Allocation Mode    : Static
DNS Negotiation      : Enabled
Local IP             : 10.7.1.200
Echo Interval        : 30
Echo Failure         : 5
=====
AP#
```

Authentication

Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point, or by using a database configured on a central RADIUS server. Alternatively, authentication can be implemented using the IEEE 802.1X network access control protocol.

The access point can also operate in a 802.1X supplicant mode. This enables the access point itself and any bridge-connected units to be authenticated with a RADIUS server using a configured MD5 user name and password. This mechanism can prevent rogue access points from gaining access to the network.

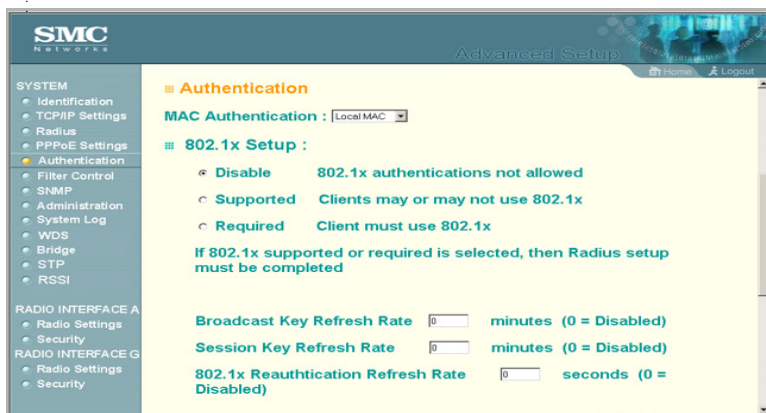


Ethernet Supplicant Setup – Allows the access point to act as an 802.1X supplicant so it can be authenticated through its Ethernet port with a RADIUS server on the local network. When enabled, a unique MD5 user name and password needs to be configured. (Default: Disabled)

- Enabled/Disabled – Enables/Disables the 802.1X supplicant function.
 - Username – Specifies the MD5 user name. (Range: 1-22 characters)
 - Password – Specifies the MD5 password. (Range: 1-22 characters)

WDS Supplicant Setup – Allows the access point to act as an 802.1X supplicant so it can be authenticated through a WDS (wireless) port with a RADIUS server on the remote network. When enabled, a unique MD5 user name and password needs to be configured for the WDS port. For a SMC2888W-S Slave unit, there is only one WDS port. For a SMC2888W-M Master unit, there are 16 WDS ports. (Default: Disabled)

System Configuration



MAC Authentication – You can configure a list of the MAC addresses for wireless clients that are authorized to access the network. This provides a basic level of authentication for wireless clients attempting to gain access to the network. A database of authorized MAC addresses can be stored locally on the access point or remotely on a central RADIUS server. (Default: Local MAC)

- **Local MAC:** The MAC address of the associating station is compared against the local database stored on the access point. The Local MAC Authentication section enables the local database to be set up.
- **Radius MAC:** The MAC address of the associating station is sent to a configured RADIUS server for authentication. When using a RADIUS authentication server for MAC address authentication, the server must first be configured in the Radius window (page 6-10).
- **Disable:** No checks are performed on an associating station's MAC address.

Note: Client station MAC authentication occurs prior to the IEEE 802.1X authentication procedure configured for the access point. However, a client's MAC address provides relatively weak user authentication, since MAC addresses can be easily captured and used by another station to break into the network. Using 802.1X provides more robust user authentication using user names and passwords or digital certificates. So, although you can configure the access point to use MAC address and 802.1X authentication together, it is better to choose one or the other, as appropriate.

802.1X Setup – IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the access point grants client access to the network.

The 802.1X EAP packets are also used to pass dynamic unicast session keys and static broadcast keys to wireless clients. Session keys are unique to each client and are used to encrypt and correlate traffic passing between a specific client and the access point. You can also enable broadcast key rotation, so the access point provides a dynamic broadcast key and changes it at a specified interval.

You can enable 802.1X as optionally supported or as required to enhance the security of the wireless network.

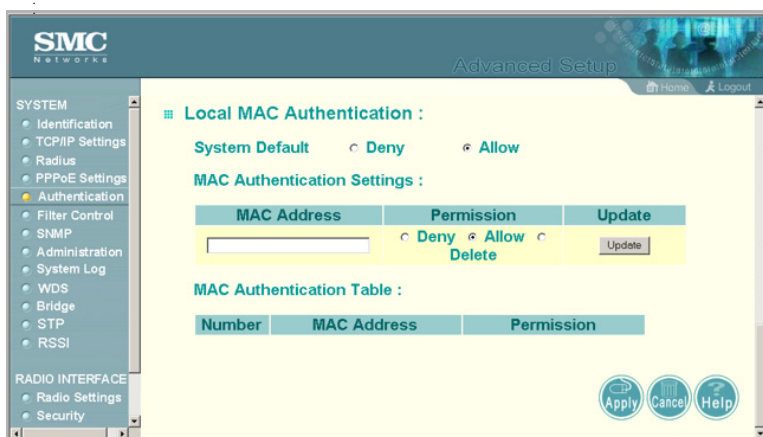
- **Disable:** The access point does not support 802.1X authentication for any wireless client. After successful wireless association with the access point, each client is allowed to access the network.

System Configuration

- **Supported:** The access point supports 802.1X authentication only for clients initiating the 802.1X authentication process (i.e., the access point does not initiate 802.1X authentication). For clients initiating 802.1X, only those successfully authenticated are allowed to access the network. For those clients not initiating 802.1X, access to the network is allowed after successful wireless association with the access point.
- **Required:** The access point enforces 802.1X authentication for all associated wireless clients. If 802.1X authentication is not initiated by a client, the access point will initiate authentication. Only those clients successfully authenticated with 802.1X are allowed to access the network.

When 802.1X is enabled, the broadcast and session key rotation intervals can also be configured.

- **Broadcast Key Refresh Rate:** Sets the interval at which the broadcast keys are refreshed for stations using 802.1X dynamic keying. (Range: 0-1440 minutes; Default: 0 means disabled)
- **Session Key Refresh Rate:** The interval at which the access point refreshes unicast session keys for associated clients. (Range: 0-1440 minutes; Default: 0 means disabled)
- **802.1X Re-authentication Refresh Rate:** The time period after which a connected client must be re-authenticated. During the re-authentication process of verifying the client's credentials on the RADIUS server, the client remains connected the network. Only if re-authentication fails is network access blocked. (Range: 0-65535 seconds; Default: 0 means disabled)



Local MAC Authentication – Configures the local MAC authentication database. The MAC database provides a mechanism to take certain actions based on a wireless client's MAC address. The MAC list can be configured to allow or deny network access to specific clients.

- **System Default:** Specifies a default action for all unknown MAC addresses (that is, those not listed in the local MAC database).
 - **Deny:** Blocks access for all MAC addresses except those listed in the local database as “Allow.”
 - **Allow:** Permits access for all MAC addresses except those listed in the local database as “Deny.”
- **MAC Authentication Settings:** Enters specified MAC addresses and permissions into the local MAC database.
 - **MAC Address:** Physical address of a client. Enter six pairs of hexadecimal digits separated by hyphens; for example, 00-90-D1-12-AB-89.

System Configuration

- **Permission:** Select Allow to permit access or Deny to block access. If Delete is selected, the specified MAC address entry is removed from the database.
- **Update:** Enters the specified MAC address and permission setting into the local database.
- **MAC Authentication Table:** Displays current entries in the local MAC database.

CLI Commands for 802.1X Supplicant Configuration – Use the **802.1X supplicant** commands to set the Ethernet and WDS user names and passwords, and to enable the feature.

```
DUAL OUTDOOR(config)#802.1X supplicant eth_user David 7-55
DUAL OUTDOOR(config)#802.1X supplicant eth_password DEF 7-55
DUAL OUTDOOR(config)#802.1X supplicant eth 7-55
DUAL OUTDOOR(config)#
```

```
DUAL OUTDOOR(config)#802.1X supplicant wds_user 1 David 7-55
DUAL OUTDOOR(config)#802.1X supplicant wds_password 1 ABC 7-55
DUAL OUTDOOR(config)#802.1X supplicant wds 1 7-55
DUAL OUTDOOR(config)#
```

CLI Commands for Local MAC Authentication – Use the **mac-authentication server** command from the global configuration mode to enable local MAC authentication. Set the default for MAC addresses not in the local table using the **address filter default** command, then enter MAC addresses in the local table using the **address filter entry** command. To remove an entry from the table, use the **address filter delete**

command. To display the current settings, use the **show authentication** command from the Exec mode.

```
AP(config)#mac-authentication server local              7-59
AP(config)#address filter default denied               7-56
AP(config)#address filter entry 00-70-50-cc-99-1a denied 7-57
AP(config)#address filter entry 00-70-50-cc-99-1b allowed
AP(config)#address filter entry 00-70-50-cc-99-1c allowed
AP(config)#address filter delete 00-70-50-cc-99-1c      7-58
AP(config)#exit
AP#show authentication                                  7-60

Authentication Information
=====
MAC Authentication Server      : LOCAL
MAC Auth Session Timeout Value : 300 secs
802.1X                         : DISABLED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1X Session Timeout Value   : 300 secs
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address      Status
-----
00-70-50-cc-99-1a  DENIED
00-70-50-cc-99-1b  ALLOWED
=====
AP#
```

System Configuration

CLI Commands for RADIUS MAC Authentication – Use the **mac-authentication server** command from the global configuration mode to enable remote MAC authentication. Set the timeout value for re-authentication using the **mac-authentication session-timeout** command. Be sure to also configure connection settings for the RADIUS server (not shown in the following example). To display the current settings, use the **show authentication** command from the Exec mode.

```
AP(config)#mac-authentication server remote                               7-59
AP(config)#mac-authentication session-timeout 300                         7-60
AP(config)#exit
AP#show authentication                                                    7-60

Authentication Information
=====
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 300 secs
802.1X                         : DISABLED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1X Session Timeout Value   : 300 secs
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address      Status
-----
00-70-50-cc-99-1a  DENIED
00-70-50-cc-99-1b  ALLOWED
=====
AP#
```

CLI Commands for 802.1X Authentication – Use the **802.1X supported** command from the global configuration mode to enable 802.1X authentication. Set the session and broadcast key refresh rate, and the re-authentication timeout. To display the current settings, use the **show authentication** command from the Exec mode.

```
AP(config)#802.1X supported                                7-51
AP(config)#802.1X broadcast-key-refresh-rate 5             7-52
AP(config)#802.1X session-key-refresh-rate 5              7-53
AP(config)#802.1X session-timeout 300                     7-54
AP(config)#exit
AP#show authentication                                     7-60

Authentication Information
=====
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 300 secs
802.1X                        : SUPPORTED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1X Session Timeout Value   : 300 secs
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address      Status
-----
00-70-50-cc-99-1a  DENIED
00-70-50-cc-99-1b  ALLOWED
=====
AP#
```

System Configuration

Filter Control

The wireless bridge can employ VLAN tagging support and network traffic frame filtering to control access to network resources and increase security.

The screenshot shows the 'Advanced Setup' page for SMC Networks. The left sidebar contains a navigation menu with categories: SYSTEM (Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, Administration, System Log, WDS, Bridge, STP, RSSI), RADIO INTERFACE A (Radio Settings, Security), and RADIO INTERFACE G (Radio Settings, Security). The 'Filter Control' section is active, showing the following settings:

- Native VLAN ID :
- VLAN : ☒ Disable ☐ Enable
- Local Bridge Filter : ☒ Disable ☐ Enable (Prevent wireless client to wireless client communication)
- AP Management Filter : ☒ Disable ☐ Enable (Prevent AP management via wireless client)
- Ethernet Type Filter : ☒ Disable ☐ Enable

Below these settings is a table with three columns: Local Management, ISO Designator, and Status.

Local Management	ISO Designator	Status
Aironet_DDP	0x872d	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Appletalk_ARP	0x80f3	<input checked="" type="radio"/> OFF <input type="radio"/> ON
ARP	0x0806	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Banyan	0x0bad	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Berkeley_Trailer_Negotiation	0x1000	<input checked="" type="radio"/> OFF <input type="radio"/> ON

Native VLAN ID – The VLAN ID assigned to wireless clients that are not assigned to a specific VLAN by RADIUS server configuration. (Range: 1-64)

VLAN – Enables or disables VLAN tagging support on the wireless bridge (changing the VLAN status forces a system reboot). When VLAN support is enabled, the wireless bridge tags traffic passing to the wired network with the assigned VLAN ID associated with each client on the RADIUS server or the configured native VLAN ID. Traffic received from the wired network must also be tagged with a known VLAN ID. Received

traffic that has an unknown VLAN ID or no VLAN tag is dropped. When VLAN support is disabled, the wireless bridge does not tag traffic passing to the wired network and ignores the VLAN tags on any received frames.

Note: Before enabling VLANs on the wireless bridge, you must configure the connected LAN switch port to accept tagged VLAN packets with the wireless bridge's native VLAN ID. Otherwise, connectivity to the wireless bridge will be lost when you enable the VLAN feature.

Up to 64 VLAN IDs can be mapped to specific wireless clients, allowing users to remain within the same VLAN as they move around a campus site. This feature can also be used to control access to network resources from wireless clients, thereby improving security.

A VLAN ID (1-4094) is assigned to a client after successful authentication using IEEE 802.1X and a central RADIUS server. The user VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the access point assigns the user to its own configured native VLAN ID.

When setting up VLAN IDs for each user on the RADIUS server, be sure to use the RADIUS attributes and values as indicated in the following table.

Number	RADIUS Attribute	Value
64	Tunnel-Type	VLAN (13)
65	Tunnel-Medium-Type	802
81	Tunnel-Private-Group	VLANID (1 to 4094 in hexadecimal)

System Configuration

Note: The specific configuration of RADIUS server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS server software.

When VLAN filtering is enabled, the access point must also have 802.1X authentication enabled and a RADIUS server configured. Wireless clients must also support 802.1X client software to be assigned to a specific VLAN.

When VLAN filtering is disabled, the access point ignores the VLAN tags on any received frames.

Local Bridge Filter – Controls wireless-to-wireless communications between clients through the access point. However, it does not affect communications between wireless clients and the wired network.

- **Disable:** Allows wireless-to-wireless communications between clients through the access point.
- **Enable:** Blocks wireless-to-wireless communications between clients through the access point.

AP Management Filter – Controls management access to the access point from wireless clients. Management interfaces include the web, Telnet, or SNMP.

- **Disable:** Allows management access from wireless clients.
- **Enable:** Blocks management access from wireless clients.

Ethernet Type Filter – Controls checks on the Ethernet type of all incoming and outgoing Ethernet packets against the protocol filtering table.

- **Disable:** Wireless bridge does not filter Ethernet protocol types.

- **Enable:** Wireless bridge filters Ethernet protocol types based on the configuration of protocol types in the filter table. If a protocol has its status set to “ON,” the protocol is filtered from the wireless bridge.

CLI Commands for VLAN Support – From the global configuration mode use the **native-vlanid** command to set the default VLAN ID for the Ethernet interface, then enable VLANs using the **vlan enable** command. When you change the access point's VLAN support setting, you must reboot the access point to implement the change. To view the current VLAN settings, use the **show system** command.

```
AP(config)#native-vlanid 3
7-125
AP(config)#vlan enable
7-124
Reboot system now? <y/n>: y
```

CLI Commands for Bridge Filtering – Use the **filter ap-manage** command to restrict management access from wireless clients. To configure Ethernet protocol filtering, use the **filter ethernet-type enable** command to enable filtering and the **filter ethernet-type protocol** command to define the protocols that

System Configuration

you want to filter. To display the current settings, use the **show filters** command from the Exec mode.

```
AP(config)#filter ap-manage 7-77
AP(config)#filter ethernet-type enable 7-78
AP(config)#filter ethernet-type protocol ARP 7-79
AP(config)#exit
AP#show filters 7-80

Protocol Filter Information
=====
AP Management :ENABLED
Ethernet Type Filter :ENABLED

Enabled Protocol Filters
-----
Protocol: ARP ISO: 0x0806
=====
AP#
```

SNMP

You can use a network management application to manage the wireless bridge via the Simple Network Management Protocol (SNMP) from a management station. To implement SNMP management, the wireless bridge must have an IP address and subnet mask, configured either manually or dynamically. Once an IP address has been configured, appropriate SNMP communities and trap receivers should be configured.

Community names are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the wireless bridge. To communicate with the wireless bridge, a management station must first submit a valid community name for authentication. You therefore need to assign community names to specified users or user groups and set the access level.

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM (containing Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, and SNMP), RADIO INTERFACE A, RADIO INTERFACE G, and Security. The main content area is titled 'SNMP' and shows a status 'SNMP : Disable' with a radio button to switch to 'Enable'. Below this are four input fields: 'Community Name (Read Only)', 'Community Name (Read/Write)', 'Trap Destination IP Address', and 'Trap Destination Community Name'. At the bottom right are three buttons: 'Apply', 'Cancel', and 'Help'.

SNMP – Enables or disables SNMP management access and also enables the wireless bridge to send SNMP traps (notifications). SNMP management is disabled by default.

Community Name (Read Only) – Defines the SNMP community access string that has read-only access. Authorized management stations are only able to retrieve MIB objects. (Maximum length: 23 characters, case sensitive; Default: public)

Community Name (Read/Write) – Defines the SNMP community access string that has read/write access. Authorized management stations are able to both retrieve and modify MIB objects. (Maximum length: 23 characters, case sensitive; Default: private)

Trap Destination IP Address – Specifies the recipient of SNMP notifications. Enter the IP address or the host name. (Host Name: 1 to 20 characters)

System Configuration

Trap Destination Community Name – The community string sent with the notification operation. (Maximum length: 23 characters; Default: public)

CLI Commands for SNMP – Use the **snmp-server enable server** command from the global configuration mode to enable SNMP. To set read/write and read-only community names, use the **snmp-server community** command. The **snmp-server host** command defines a trap receiver host. To view the current SNMP settings, use the **show snmp** command.

```
AP(config)#snmp-server enable server                                7-36
AP(config)#snmp-server community alpha rw                          7-34
AP(config)#snmp-server community beta ro
AP(config)#snmp-server host 10.1.19.23 alpha                        7-37
AP(config)#exit
AP#show snmp                                                        7-39

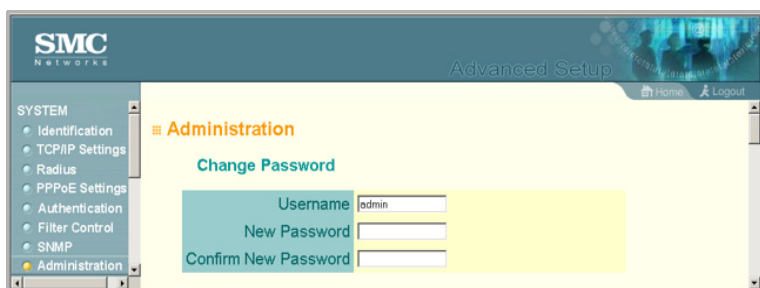
SNMP Information
=====
Service State   : Enable
Community (ro)  : ****
Community (rw)  : *****
Location       : building-1
Contact        : Paul
Traps          : Enabled
Host Name/IP    : 10.1.19.23
Trap Community  : *****
=====
AP#
```

Administration

Changing the Password

Management access to the web and CLI interface on the wireless bridge is controlled through a single user name and password. You can also gain additional access security by using control filters (see “Filter Control” on page 6-26).

To protect access to the management interface, you need to configure an Administrator’s user name and password as soon as possible. If the user name and password are not configured, then anyone having access to the wireless bridge may be able to compromise wireless bridge and network security.



The screenshot displays the SMC Networks Advanced Setup web interface. On the left is a navigation menu under the 'SYSTEM' heading, listing: Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, and Administration (which is highlighted with a yellow background). The main content area is titled 'Administration' in orange. Below this, the 'Change Password' section is shown. It contains three input fields: 'Username' with the value 'admin', 'New Password', and 'Confirm New Password'. The interface has a blue header with the SMC Networks logo and 'Advanced Setup' text, and a top right corner with 'Home' and 'Logout' links.

Username – The name of the user. The default name is “admin.” (Length: 3-16 characters, case sensitive.)

New Password – The password for management access. (Length: 3-16 characters, case sensitive)

Confirm New Password – Enter the password again for verification.

System Configuration

CLI Commands for the User Name and Password – Use the **username** and **password** commands from the CLI configuration mode.

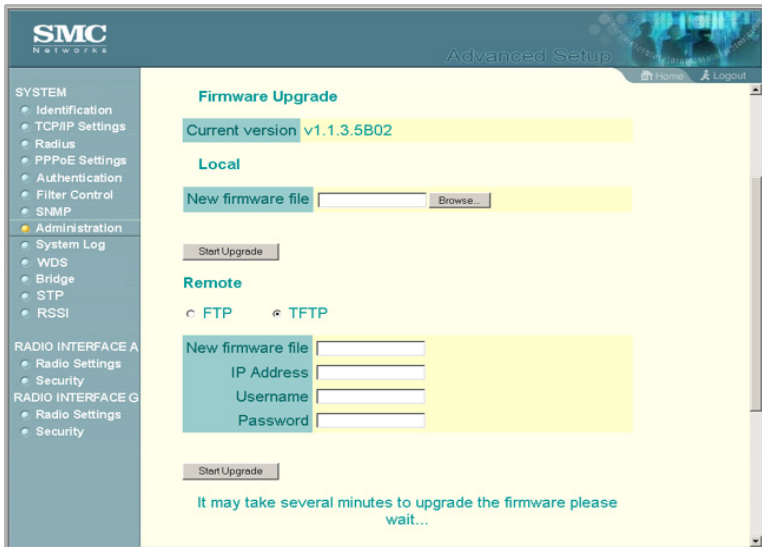
AP(config)#username bob	7-19
AP(config)#password spiderman	7-20
AP#	

Upgrading Firmware

You can upgrade new wireless bridge software from a local file on the management workstation, or from an FTP or TFTP server.

After upgrading new software, you must reboot the wireless bridge to implement the new code. Until a reboot occurs, the wireless bridge will continue to run the software it was using before the upgrade started. Also note that rebooting the wireless bridge with new software will reset the configuration to the factory default settings.

Note: Before upgrading your wireless bridge software, it is recommended to save a copy of the current configuration file. See “copy” on page 7-41 for information on saving the configuration file to a TFTP or FTP server.



Before upgrading new software, verify that the wireless bridge is connected to the network and has been configured with a compatible IP address and subnet mask.

If you need to download from an FTP or TFTP server, take the following additional steps:

- Obtain the IP address of the FTP or TFTP server where the wireless bridge software is stored.
- If upgrading from an FTP server, be sure that you have an account configured on the server with a user name and password.

Current version – Version number of runtime code.

System Configuration

Firmware Upgrade Local – Downloads an operation code image file from the web management station to the wireless bridge using HTTP. Use the Browse button to locate the image file locally on the management station and click Start Upgrade to proceed.

- **New firmware file:** Specifies the name of the code file on the server. The new firmware file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters for files on the wireless bridge. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Firmware Upgrade Remote – Downloads an operation code image file from a specified remote FTP or TFTP server. After filling in the following fields, click Start Upgrade to proceed.

- **New firmware file:** Specifies the name of the code file on the server. The new firmware file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the wireless bridge. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- **IP Address:** IP address or host name of FTP or TFTP server.
- **Username:** The user ID used for login on an FTP server.
- **Password:** The password used for login on an FTP server.

Restore Factory Settings – Click the Restore button to reset the configuration settings for the wireless bridge to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to re-enter the default user name (smcadmin) to re-gain management access to this device.

Reset wireless bridge – Click the Reset button to reboot the system.

Note: If you have upgraded system software, then you must reboot the wireless bridge to implement the new operation code.

CLI Commands for Downloading Software from a TFTP Server – Use the **copy tftp file** command from the Exec mode and then specify the file type, name, and IP address of the TFTP server. When the download is complete, the **dir** command can be used to check that the new file is present in the wireless bridge file system. To run the new software, use the **reset board** command to reboot the wireless bridge.

```
AP#copy tftp file7-41
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:1
TFTP Source file name:bridge-img.bin
TFTP Server IP:192.168.1.19

AP#dir7-43
File Name                               Type      File Size
-----
dfilt-img.bin                           2          1319939
bridge-img.bin                           2          1629577
syscfg                                  5           17776
syscfg_bak                              5           17776

      262144 byte(s) available

AP#reset board7-13
Reboot system now? <y/n>: y
```

System Configuration

System Log

The wireless bridge can be configured to send event and error messages to a System Log Server. The system clock can also be synchronized with a time server, so that all the messages sent to the Syslog server are stamped with the correct time and date.

The screenshot shows the 'Advanced Setup' interface for a wireless bridge, specifically the 'System Log' configuration page. The left sidebar contains a navigation menu with categories: SYSTEM (Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, Administration, System Log), RADIO INTERFACE A (Radio Settings, Security), and RADIO INTERFACE G (Radio Settings, Security). The 'System Log' section is expanded. The main content area has a title 'System Log' and a 'System Log Setup' section with radio buttons for 'Disable' and 'Enable' (currently 'Enable' is selected). Below this are three rows: 'Logging Host' with a 'Server Name / IP' text box containing '0.0.0.0', 'Logging Console' with radio buttons for 'Disable' and 'Enable' (currently 'Enable' is selected), and 'Logging Level' with a dropdown menu set to 'Error'. The 'SNTP Server' section has radio buttons for 'Disable' and 'Enable' (currently 'Enable' is selected), followed by 'Primary Server' and 'Secondary Server' text boxes containing '127.92.140.80' and '192.43.244.18' respectively. The 'Set Time Zone' section has a dropdown menu set to '(GMT-05) Eastern Time (US & Canada)', a checkbox for 'Enable Daylight Saving' which is unchecked, and a 'From' section with dropdowns for 'JAN', '1', and 'To' section with dropdowns for 'JAN', '1'.

Enabling System Logging

The wireless bridge supports a logging process that can control error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating wireless bridge and network problems.

System Log Setup – Enables the logging of error messages.

Logging Host – Enables the sending of log messages to a Syslog server host.

Server Name/IP – The IP address or name of a Syslog server.

Logging Console – Enables the logging of error messages to the console.

Logging Level – Sets the minimum severity level for event logging.

The system allows you to limit the messages that are logged by specifying a minimum severity level. The following table lists the error message levels from the most severe (Emergency) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Emergency level.

Error Level	Description
Emergency	System unusable
Alert	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

Note: The wireless bridge error log can be viewed using the Event Logs window in the Status section (page 6-92). The Event Logs window displays the last 128 messages logged in chronological order, from the newest to the oldest. Log messages saved in the wireless bridge's memory are erased when the device is rebooted.

System Configuration

CLI Commands for System Logging – To enable logging on the wireless bridge, use the **logging on** command from the global configuration mode. The **logging level** command sets the minimum level of message to log. Use the **logging console** command to enable logging to the console. Use the **logging host** command to specify up to four Syslog servers. The CLI also allows the **logging facility-type** command to set the facility-type number to use on the Syslog server. To view the current logging settings, use the **show logging** command.

```
AP(config)#logging on 7-24
AP(config)#logging level alert 7-25
AP(config)#logging console 7-25
AP(config)#logging host 1 10.1.0.3 514 7-24
AP(config)#logging facility-type 19 7-26
AP(config)#exit
AP#show logging 7-27

Logging Information
=====
Syslog State : Enabled
Logging Host State : Enabled
Logging Console State : Enabled
Server Domain name/IP : 1 10.1.0.3
Logging Level : Error
Logging Facility Type : 16
=====

AP#
```

Configuring SNTP

Simple Network Time Protocol (SNTP) allows the wireless bridge to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the wireless bridge enables the system log to record meaningful dates and times for event entries. If the clock is not set, the wireless bridge will only record the time from the factory default set at the last bootup.

The wireless bridge acts as an SNTP client, periodically sending time synchronization requests to specific time servers. You can configure up to two time server IP addresses. The wireless bridge will attempt to poll each server in the configured sequence.

SNTP Server – Configures the wireless bridge to operate as an SNTP client. When enabled, at least one time server IP address must be specified.

- **Primary Server:** The IP address of an SNTP or NTP time server that the wireless bridge attempts to poll for a time update.
- **Secondary Server:** The IP address of a secondary SNTP or NTP time server. The wireless bridge first attempts to update the time from the primary server; if this fails it attempts an update from the secondary server.

Note: The wireless bridge also allows you to disable SNTP and set the system clock manually using the CLI.

Set Time Zone – SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours your time zone is located before (east) or after (west) UTC.

Enable Daylight Saving – The wireless bridge provides a way to automatically adjust the system clock for Daylight Savings Time changes. To use this feature you must define the month and date to begin and to end the change from standard time. During this period the system clock is set back by one hour.

System Configuration

CLI Commands for SNTP – To enable SNTP support on the wireless bridge, from the global configuration mode specify SNTP server IP addresses using the **sntp-server ip** command, then use the **sntp-server enable** command to enable the service. Use the **sntp-server timezone** command to set the location time zone and the **sntp-server daylight-saving** command to set up a daylight saving. To view the current SNTP settings, use the **show sntp** command.

```
AP(config)#sntp-server ip 10.1.0.19                                7-29
AP(config)#sntp-server enable                                    7-30
AP(config)#sntp-server timezone +8                              7-32
AP(config)#sntp-server daylight-saving                          7-31
Enter Daylight saving from which month<1-12>: 3
and which day<1-31>: 31
Enter Daylight saving end to which month<1-12>: 10
and which day<1-31>: 31
AP(config)#exit
AP#show sntp                                                    7-33

SNTP Information
=====
Service State           : Enabled
SNTP (server 1) IP      : 137.92.140.80
SNTP (server 2) IP      : 192.43.244.18
Current Time            : 19 : 35, Oct 10th, 2003
Time Zone               : +8 (TAIPEI, BEIJING)
Daylight Saving         : Enabled, from Mar, 31th to Oct, 31th
=====
AP#
```

CLI Commands for the System Clock – The following example shows how to manually set the system time when SNTP server support is disabled on the wireless bridge.

```
AP(config)#no sntp-server enable                                7-30
AP(config)#sntp-server date-time                                7-31
Enter Year<1970-2100>: 2003
Enter Month<1-12>: 10
Enter Day<1-31>: 10
Enter Hour<0-23>: 18
Enter Min<0-59>: 35
AP(config)#
```

Wireless Distribution System (WDS)

The IEEE 802.11 standard defines a Wireless Distribution System (WDS) for connections between wireless bridges. The access point uses WDS to forward traffic on bridge links between units. When using WDS, only wireless bridge units can associate to each other using the bridge band. A wireless client cannot associate with the access point on the wireless bridge band.

To set up a wireless bridge link, you must configure the WDS forwarding table by specifying the **Ethernet MAC Address** of the bridge to which you want to forward traffic. For a Slave bridge unit, you need to specify the MAC address of the wireless bridge unit at the opposite end of the link. For a Master bridge unit, you need to specify the MAC addresses of all the Slave bridge units in the network. When trying to connect to other bridges, please input the **Ethernet MAC Address**.

The screenshot displays the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM (including Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, Administration, and System Log), WDS (highlighted with a yellow star, including Bridge, STP, and RSSI), RADIO INTERFACE A (including Radio Settings and Security), and RADIO INTERFACE G (including Radio Settings and Security). The main content area is titled 'Port / Mac Pair Settings' and 'Master Mode'. It contains a table with 10 rows, each representing a port and its associated MAC address and status.

Port No	Mac	Status
1	0F:00:22:44:99:0F	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
2	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
3	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
4	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
5	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
6	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
7	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
8	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
9	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
10	00:00:00:00:00:00	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

System Configuration



Mode – The wireless bridge is set to operate as a Slave or Master unit:

- **Master Mode:** In a point-to-multipoint network configuration, only one wireless bridge unit must be a Master unit (all others must be Slave units). A Master wireless bridge provides support for up to 16 MAC addresses in the WDS forwarding table. The MAC addresses of all other Slave bridge units in the network must be configured in the forwarding table.
- **Slave Mode:** A Slave wireless bridge provides support for only one MAC address in the WDS forwarding table. A Slave bridge communicates with only one other wireless bridge, either another Slave bridge in a point-to-point configuration, or to the Master bridge in a point-to-multipoint configuration.

Port Number (Master bridge only) – The wireless port identifier.

MAC Address – The physical layer address of the wireless bridge unit at the other end of the wireless link. (12 hexadecimal digits in the form “xx:xx:xx:xx:xx:xx”)

Port Status – Enables or disables the wireless bridge link.

Note: The Ethernet MAC address for each bridge unit is printed on the label on the back of the unit.

CLI Commands for WDS – The following example shows how to configure the MAC address of the wireless bridge at the opposite end of a point-to-point link, and then enable forwarding on the link.

```
AP(config)#wds mac-address 1 00-12-34-56-78-9a      7-62
AP(config)#wds enable                               7-63
AP(config)#exit
AP#show wds                                          7-64
```

Outdoor_Mode		:	SLAVE
=====			
Port ID		Status	Mac-Address
=====			
01		ENABLE	00-12-34-56-78-9A
=====			

AP#

Bridge

The wireless bridge can store the MAC addresses for all known devices in the connected networks. All the addresses are learned by monitoring traffic received by the wireless bridge and are stored in a dynamic MAC address table. This information is then used to forward traffic directly between the Ethernet port and the corresponding wireless interface.

The Bridging page allows the MAC address aging time to be set for both the Ethernet port and the bridge radio interface. If the MAC address of an entry in the address table is not seen on the associated interface for longer than the aging time, the entry is discarded.

System Configuration

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM, RADIO INTERFACE A, and RADIO INTERFACE G. The 'Bridge' option under SYSTEM is selected. The main content area is titled 'Bridge Ageing Time' and contains two rows of configuration fields. The first row is for 'Ethernet' with a value of '100 sec'. The second row is for 'Wireless 802.11a' with a value of '1800 sec'. At the bottom right of the main area are three circular buttons: 'Apply', 'Cancel', and 'Help'.

Bridge Ageing Time	
Ethernet	100 sec
Wireless 802.11a	1800 sec

Bridge Aging Time – Changes the aging time for entries in the dynamic address table:

- Ethernet: The time after which a learned Ethernet port entry is discarded. (Range: 60-1800 seconds; Default: 100 seconds)
- Wireless 802.11a (g): The time after which a learned wireless entry is discarded. (Range: 60-1800 seconds; Default: 1800 seconds)

CLI Commands for Bridging – The following example shows how to set the MAC address aging time for the wireless bridge.

```
AP(config)#bridge timeout 0 300                                7-66
AP(config)#bridge timeout 2 1000                                7-66
AP(config)#exit
AP#show bridge                                                  7-75
```



```

          Bridge Information
=====
Media Type | Age Time(sec) |
=====
  Ethernet |      300      |
   WLAN_A  |     1000      |
=====
```



```

Bridge Id           : 32768.037fbef192
Root Bridge Id      : 32768.01f47483e2
Root Path Cost       : 25
Root Port Id        : 0
Bridge Status        : Enabled
Bridge Priority       : 32768
Bridge Hello Time    : 2 Seconds
Bridge Maximum Age   : 20 Seconds
Bridge Forward Delay : 15 Seconds
===== Port Summary
=====
```

Id	Priority	Path Cost	Fast Forward	Status	State
0	128	25	Enable	Enabled	Forwarding

```
AP#
```

Spanning Tree Protocol (STP)

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the wireless bridge to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging

System Configuration

device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the root bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM, RADIO INTERFACE A, and RADIO INTERFACE G. The main content area is titled 'Spanning Tree Protocol' and includes a checkbox for 'Enable' which is checked. Below this are four configuration fields: 'Forward Delay (4-30)' set to 15, 'Hello Time (1-10)' set to 2, 'Max Age (6-40)' set to 20, and 'Bridge Priority (1-65535)' set to 32768. The 'Ethernet' section contains three fields: 'Port Cost (1-65535)' set to 19, 'Priority (1-255)' set to 128, and 'Port Fast' set to 'Disable'. The 'Wireless' section contains a table with 5 columns: Port No, Path Cost (1-65535), Priority (1-255), Port Fast, and Status. The table has two rows, both with Port No 1 and 2, Path Cost 40, Priority 128, Port Fast set to 'Disable', and Status set to 'Disable'.

Port No	Path Cost (1-65535)	Priority (1-255)	Port Fast	Status
1	40	128	Disable	Disable
2	40	128	Disable	Disable

Enable – Enables/disables STP on the wireless bridge. (Default: Enabled)

Forward Delay – The maximum time (in seconds) this device waits before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result. (Range: 4-30 seconds)

- Default: 15
- Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$
- Maximum: 30

System Configuration

Hello Time – Interval (in seconds) at which the root device transmits a configuration message. (Range: 1-10 seconds)

- Default: 2
- Minimum: 1
- Maximum: The lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$

Maximum Age – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (Range: 6-40 seconds)

- Default: 20
- Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$.
- Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$

Bridge Priority – Used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)

- Range: 0-65535
- Default: 32768

Port Cost – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values

assigned to ports with slower media. (Path cost takes precedence over port priority.)

- Range: 1-65535
- Default: Ethernet interface: 19; Wireless interface: 40

Priority – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

- Default: 128
- Range: 0-240, in steps of 16

System Configuration

Port Fast (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying fast forwarding provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that fast forwarding should only be enabled for ports connected to an end-node device. (Default: Disabled)

Status – Enables/disables STP on this interface. (Default: Enabled)

CLI Commands for STP – The following example configures spanning tree parameters for the bridge and wireless port 5.

```
AP(config)#bridge stp-bridge priority 40000 7-70
AP(config)#bridge stp-bridge hello-time 5 7-68
AP(config)#bridge stp-bridge max-age 38 7-69
AP(config)#bridge stp-bridge forward-time 20 7-67
AP(config)#no bridge stp-port spanning-disabled 5 7-74
AP(config)#bridge stp-port priority 5 0 7-72
AP(config)#bridge stp-port path-cost 5 50 7-71
AP(config)#no bridge stp-port portfast 5 7-73
AP(config)#end
AP#show bridge 7-75
```

Bridge Information

```
=====
Media Type | Age Time(sec) |
=====
Ethernet   | 300             |
WLAN_A     | 1000            |
=====
```

Bridge Id : 32768.037fbef192
Root Bridge Id : 32768.01f47483e2
Root Path Cost : 25
Root Port Id : 0
Bridge Status : Enabled
Bridge Priority : 40000
Bridge Hello Time : 5 Seconds
Bridge Maximum Age : 38 Seconds
Bridge Forward Delay: 20 Seconds

===== Port Summary

Id	Priority	Path Cost	Fast Forward	Status	State
0	128	25	Enable	Enabled	Forwarding

AP#

System Configuration

RSSI

The RSSI value displayed on the RSSI page represents a signal to noise ratio. A value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold. This value can be used to align antennas (see page 4-9) and monitor the quality of the received signal for bridge links. An RSSI value of about 30 or more indicates a strong enough signal to support the maximum data rate of 54 Mbps. Below a value of 30, the supported data rate would drop to lower rates. A value of 15 or less indicates that the signal is weak and the antennas may require realignment.

The RSSI controls allow the external connector to be disabled and the receive signal for each WDS port displayed.

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: SYSTEM (Identification, TCP/IP Settings, Radius, PPPoE Settings, Authentication, Filter Control, SNMP, Administration, System Log, WDS, Bridge, STP, RSSI), RADIO INTERFACE A (Radio Settings, Security), and RADIO INTERFACE B (Radio Settings, Security). The main content area is titled "RSSI" and contains two sections: "Output Activate" and "Distance".

Output Activate	
Output Activate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Port Number	<input type="text"/>
Output Value	<input type="text"/>

Distance	
Mode	<input checked="" type="radio"/> Normal <input type="radio"/> Turbo
Distance	<input type="text"/> KM

At the bottom right of the page are three buttons: Apply, Cancel, and Help.

RSSI – The RSSI value for a selected port can be displayed and a representative voltage output can be enabled.

- **Output Activate:** Enables or disables the RSSI voltage output on the external RSSI connector. (Default: Enabled)
- **Port Number:** Selects a specific WDS port for which to set the maximum RSSI output voltage level. Ports 1-16 are available for a Master unit, only port 1 for a Slave unit. (Default: 1)
- **Output Value:** The maximum RSSI voltage level for the current selected WDS port. A value of zero indicates that there is no received signal or that the WDS port is disabled.

Distance – This value is used to adjust timeout values to take into account transmit delays due to link distances in the wireless bridge network. For a point-to-point link, specify the approximate distance between the two bridges. For a point-to-multipoint network, specify the distance of the Slave bridge farthest from the Master bridge

- **Mode:** Indicates if the 802.11a radio is operating in normal or Turbo mode. (See "Radio Settings A" on page 6-57.)
- **Distance:** The approximate distance between antennas in a bridge link.

Note: There are currently no equivalent CLI commands for the RSSI controls.

Radio Interface

The IEEE 802.11a and 802.11g interfaces include configuration options for radio signal characteristics and wireless security features. The configuration options are nearly identical, but depend on which interface is operating as the bridge band. Both interfaces and operating modes are covered in this section of the manual.

The access point can operate in the following modes:

- 802.11a in bridge mode and 802.11g in access point mode
- 802.11a in access point mode and 802.11g in bridge mode
- 802.11a and 802.11g both in access point mode (no bridging)
- 802.11a only in bridge or access point mode
- 802.11g only in bridge or access point mode

Note that 802.11g is backward compatible with 802.11b and can be configured to support both client types or restricted to 802.11g clients only. Both wireless interfaces are configured independently under the following web pages:

- Radio Interface A: 802.11a
- Radio Interface G: 802.11b/g

Note: The radio channel settings for the wireless bridge are limited by local regulations, which determine the number of channels that are available.

Radio Settings A (802.11a)

The IEEE 802.11a interface operates within the 5 GHz band, at up to 54 Mbps in normal mode or up to 108 Mbps in Turbo mode.

SMC Networks Advanced Setup

SYSTEM

- Identification
- TCP/IP Settings
- Radius
- PPPoE Settings
- Authentication
- Filter Control
- SNMP
- Administration
- System Log
- WDS
- Bridge
- STP
- RSSI

RADIO INTERFACE A

- Radio Settings

RADIO INTERFACE G

- Radio Settings
- Security

802.11a:

Radio Settings

"Before enabling the radios you must set the country selection via the CLI."

☐ **Enable**

Description : Enterprise 802.11a Wireless Outdoor Bridge/AP

Network Name (SSID) : SMC

Secure Access : ☐ Disable ☒ Enable

Radio Channel : There's no 11a channel supported by this country.

Auto Channel Select : ☒ Disable ☐ Enable

Transmit Power 100%

Maximum Supported Rate: 54 Mbps

Beacon Interval (20-1000) 100 TUs

Data Beacon Rate (DTIM) (1-255) 1 Beacons

Fragment Length (256-2346) 2346 Bytes

RTS Threshold (0-2347) 2347 Bytes

Apply **Cancel** **Help**

Enable – Enables radio communications on the wireless interface. (Default: Enabled)

Description – Adds a comment or description to the wireless interface. (Range: 1-80 characters)

Network Name (SSID) – (Access point mode only) The name of the basic service set provided by the access point. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point. (Default: SMC; Range: 1-32 characters)

Note: The SSID is not configurable when the radio band is set to Bridge

System Configuration

mode.

SSID Broadcast – When enabled, the access point radio does not include its SSID in beacon messages. Nor does it respond to probe requests from clients that do not include a fixed SSID. (Default: Disable)

Turbo Mode – The normal 802.11a wireless operation mode provides connections up to 54 Mbps. Turbo Mode is an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps. Enabling Turbo Mode allows the wireless bridge to provide connections up to 108 Mbps. (Default: Disabled)

Note: In normal mode, the wireless bridge provides a channel bandwidth of 20 MHz, and supports the maximum number of channels permitted by local regulations (e.g., 11 channels for the United States). In Turbo Mode, the channel bandwidth is increased to 40 MHz to support the increased data rate. However, this reduces the number of channels supported (e.g., 5 channels for the United States).

Radio Channel – The radio channel that the wireless bridge uses to communicate with wireless clients. When multiple wireless bridges are deployed in the same area, set the channel on neighboring wireless bridges at least four channels apart to avoid interference with each other. For example, in the United States you can deploy up to four wireless bridges in the same area (e.g., channels 36, 56, 149, 165). Also note that the channel for wireless clients is automatically set to the same as that used by the wireless bridge to which it is linked. (Default: Channel 60 for normal mode, and channel 42 for Turbo mode)

Normal Mode

60 ch, 5.300 GHz	▼
44 ch, 5.220 GHz	▲
48 ch, 5.240 GHz	
52 ch, 5.260 GHz	
56 ch, 5.280 GHz	
60 ch, 5.300 GHz	
64 ch, 5.320 GHz	
149 ch, 5.745 GHz	
153 ch, 5.765 GHz	
157 ch, 5.785 GHz	
161 ch, 5.805 GHz	
165 ch, 5.825 GHz	▼

Turbo Mode

42 ch, 5.210 GHz	▼
42 ch, 5.210 GHz	
50 ch, 5.250 GHz	
58 ch, 5.290 GHz	
152 ch, 5.760 GHz	
160 ch, 5.800 GHz	

Auto Channel Select – Enables the wireless bridge to automatically select an unoccupied radio channel. (Default: Enabled)

Transmit Power – Adjusts the power of the radio signals transmitted from the wireless bridge. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Options: 100%, 50%, 25%, 12%, minimum; Default: 100%)

Maximum Supported Rate – The maximum data rate at which the access point transmits unicast packets on the wireless interface. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Options: 54, 48, 36, 24, 18, 12, 9, 6 Mbps; Default: 54 Mbps)

Beacon Interval – The rate at which beacon signals are transmitted from the wireless bridge. The beacon signals allow wireless clients to maintain contact with the wireless bridge. They may also carry power-management information. (Range: 20-1000 TUs; Default: 100 TUs)

Data Beacon Rate – The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

Known also as the Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of 2 indicates that the wireless bridge will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster.

System Configuration

Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames.

(Range: 1-255 beacons; Default: 2 beacons)

Fragment Length – Configures the minimum packet size that can be fragmented when passing through the wireless bridge.

Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)

RTS Threshold – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The wireless bridge sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 0, the wireless bridge always sends RTS signals. If set to 2347, the wireless bridge never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The wireless bridges contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 0-2347 bytes; Default: 2347 bytes)

Maximum Associations – (Access point mode only) Sets the maximum number of clients that can be associated with the access point radio at the same time.

(Range: 1-64 per radio: Default: 64)

CLI Commands for the 802.11a Wireless Interface – From the global configuration mode, enter the **interface wireless a** command to access the 802.11a radio interface. If required, configure a name for the interface using the **description** command. Use the **turbo** command to enable this feature before setting the radio channel with the **channel** command. Set any other parameters as required. To view the current 802.11a radio settings, use the **show interface wireless a** command.

System Configuration

AP(config)#interface wireless a	7-99
Enter Wireless configuration commands, one per line.	
AP(if-wireless a)#description RD-AP#3	7-99
AP(if-wireless a)#ssid r&d	7-100
AP(if-wireless a)#no turbo	7-103
AP(if-wireless a)#channel 44	7-102
AP(if-wireless a)#closed-system	7-101
AP(if-wireless a)#transmit-power full	7-107
AP(if-wireless a)#speed 9	7-101
AP(if-wireless a)#max-association 32	7-108
AP(if-wireless a)#beacon-interval 150	7-104
AP(if-wireless a)#dtim-period 5	7-104
AP(if-wireless a)#fragmentation-length 512	7-105
AP(if-wireless a)#rts-threshold 256	7-106
AP(if-wireless a)#exit	
AP#show interface wireless a	7-120
Wireless Interface Information	
=====	
-----Identification-----	
Description	: RD-AP#3
Service Type	: Access Point
SSID	: r&d
Turbo Mode	: OFF
Channel	: 44
Status	: Disable
-----802.11 Parameters-----	
Transmit Power	: FULL (15 dBm)
Max Station Data Rate	: 9Mbps
Fragmentation Threshold	: 512 bytes
RTS Threshold	: 256 bytes
Beacon Interval	: 150 TUs
DTIM Interval	: 5 beacons
Maximum Association	: 32 stations
-----Security-----	
Closed System	: ENABLED
Multicast cipher	: WEP
Unicast cipher	: WEP
WPA clients	: SUPPORTED
WPA Key Mgmt Mode	: DYNAMIC
WPA PSK Key Type	: HEX
Encryption	: DISABLED
Default Transmit Key	: 1
Static Keys :	
Key 1: EMPTY	Key 2: EMPTY
Key 3: EMPTY	Key 4: EMPTY
Authentication Type	: OPEN
=====	
AP#	

Radio Settings G (802.11g)

The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Also note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

SMC Networks Advanced Setup Home Logout

SYSTEM

- Identification
- TCP/IP Settings
- Radius
- PPPoE Settings
- Authentication
- Filter Control
- SNMP
- Administration
- System Log
- WDS
- Bridge
- STP
- RSSI

RADIO INTERFACE A

- Radio Settings
- Security

RADIO INTERFACE G

- Radio Settings
- Security

802.11g:

Radio Settings

"Before enabling the radios you must set the country selection via the CLI."

☐ **Enable**

Description : Enterprise 802.11b/g Wireless Outdoor Bridge/AP

Network Name (SSID) : SMC

Secure Access : ☒ Disable ☐ Enable

Radio Channel : There's no 11g channel supported by this country.

Auto Channel Select : ☐ Disable ☒ Enable

Working Mode : ☒ b & g mixed mode ☐ g only mode ☐ b only mode

Transmit Power : 100%

Maximum Station Data Rate : 54 Mbps

Beacon Interval (20-1000) : 100 TUs

Data Beacon Rate (DTIM) (1-255) : 1 Beacons

Fragment Length (256-2346) : 2346 Bytes

RTS Threshold (0-2347) : 2347 Bytes

Maximum Associations (0-64) : 64 Clients

Enable – Enables radio communications on the access point.
(Default: Enabled)

Radio Channel – The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference

System Configuration

with each other. For example, in the United States you can deploy up to three access points in the same area (e.g., channels 1, 6, 11). Also note that the channel for wireless clients is automatically set to the same as that used by the access point to which it is linked. (Range: 1-11 (US/Canada); Default: 1)

Auto Channel Select – Enables the access point to automatically select an unoccupied radio channel. (Default: Enabled)

Working Mode – Selects the operating mode for the 802.11g wireless interface. (Default: b & g mixed mode)

- b & g mixed mode: Both 802.11b and 802.11g clients can communicate with the access point (up to 54 Mbps).
- g only: Only 802.11g clients can communicate with the access point (up to 54 Mbps).
- b only: Both 802.11b and 802.11g clients can communicate with the access point, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).

Maximum Station Data Rate – The maximum data rate at which the access point transmits unicast packets on the wireless interface. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Default: 54 Mbps)

For a description of the remaining configuration items, see “Radio Settings A (802.11a)” on page 6-57.

CLI Commands for the 802.11g Wireless Interface – From the global configuration mode, enter the **interface wireless g** command to access the 802.11g radio interface. Set the interface SSID using the **ssid** command and, if required, configure a name for the interface using the **description** command. You can also use the **closed-system** command to



stop sending the SSID in beacon messages. Select a radio channel or set selection to Auto using the **channel** command. Set any other parameters as required. To view the current 802.11g radio settings, use the **show interface wireless g** command.

```
AP(config)#interface wireless g                                7-99
Enter Wireless configuration commands, one per line.
AP(if-wireless g)#description RD-AP#3                          7-99
AP(if-wireless g)#ssid r&d                                     7-100
AP(if-wireless g)#channel auto                                  7-102
AP(if-wireless a)#closed-system                                 7-101
AP(if-wireless a)#transmit-power full                           7-107
AP(if-wireless g)#speed 6                                       7-101
AP(if-wireless g)#max-association 32                           7-108
AP(if-wireless g)#beacon-interval 150                          7-104
AP(if-wireless g)#dtim-period 5                                7-104
AP(if-wireless g)#fragmentation-length 512                     7-105
AP(if-wireless g)#rts-threshold 256                             7-106
AP(if-wireless g)#exit
AP#show interface wireless g                                    7-120
Wireless Interface Information
=====
-----Identification-----
Description                : Enterprise 802.11g Wireless Outdoor
Bridge/AP
Service Type               : Access Point
SSID                       : r&d
Channel                    : 11 (AUTO)
Status                     : Enable
-----802.11 Parameters-----
Transmit Power             : FULL (14 dBm)
Max Station Data Rate      : 6Mbps
Fragmentation Threshold    : 512 bytes
RTS Threshold              : 256 bytes
Beacon Interval            : 150 TUs
DTIM Interval              : 5 beacons
Maximum Association        : 64 stations
-----Security-----
Closed System              : DISABLED
Multicast cipher           : WEP
Unicast cipher             : TKIP
WPA clients                : SUPPORTED
WPA Key Mgmt Mode          : DYNAMIC
WPA PSK Key Type           : HEX
Encryption                 : DISABLED
Default Transmit Key       : 1
Static Keys :
    Key 1: EMPTY    Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
Authentication Type        : OPEN
=====
AP#
```

Security (Bridge Mode)

Wired Equivalent Privacy (WEP) and Advanced Encryption Standard (AES) are implemented for security in bridge mode to prevent unauthorized access to network data. To secure bridge link data transmissions, enable WEP or AES encryption for the bridge radio and set at least one encryption key.

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless bridge units. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually configured on all units in the wireless bridge network.

SMC
Networks

Advanced Setup

Home Logout

SYSTEM

- Identification
- TCP/IP Settings
- Radius
- PPPoE Settings
- Authentication
- Filter Control
- SNMP
- Administration
- System Log
- WDS
- Bridge
- STP
- RSSI

RADIO INTERFACE A

- Radio Settings
- Security

RADIO INTERFACE G

- Radio Settings
- Security

802.11a:

Security

Data Encryption (a) Setup

DisableEnable

WEP

AES

Shared Key Setup

64 Bit128 Bit152 Bit

Key Type

Hexadecimal

For 64 Bit enter 10 digits, for 128 Bit enter 26 digits, for 152 Bit enter 32 digits

Alphanumeric

For 64 Bit enter 5 characters, for 128 Bit enter 13 characters, for 152 Bit enter 16 characters

Key Number	Transmit Key Select	Key
Key 1	Hexadecimal	
Key 2	Alphanumeric	
Key 3	Alphanumeric	
Key 4	Alphanumeric	

Apply

Cancel

Help

Setting up IEEE 802.11 Wired Equivalent Privacy (WEP) shared keys prevents unauthorized access to the wireless bridge network.

Be sure to define at least one static WEP key for data encryption. Also, be sure that the WEP keys are the same for all bridge units in the wireless network.

Data Encryption Setup – Enable or disable the wireless bridge to use either WEP or AES for data encryption. If WEP encryption is selected and enabled, you must configure at least one encryption key on the wireless bridge. (Default: Disable)

Shared Key Setup – Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of WEP encryption key must be set on all bridge units in the wireless network. (Default: 128 Bit)

Key Type – Select the preferred method of entering WEP encryption keys on the wireless bridge and enter up to four keys:

- **Hexadecimal:** Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys.
- **Alphanumeric:** Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys, or 16 alphanumeric characters for 152 bit keys.
- **Transmit Key Select:** Selects the key number to use for encryption. Bridge units in the wireless network must have all four keys configured to the same values.

Note: Key index and type must match on all bridge units in the wireless network.

System Configuration

Advanced Encryption Standard (AES)

AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 security standard.

The bridge radio band uses 128-bit static AES keys (hexadecimal or alphanumeric strings) that are configured for each link pair in the wireless bridge network. For a Slave bridge unit, only one encryption key needs to be defined. A Master bridge allows a different key to be defined for each wireless bridge link in the network.

The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following sections:

- SYSTEM
 - Identification
 - TCP/IP Settings
 - Radius
 - PPPoE Settings
 - Authentication
 - Filter Control
 - SNMP
 - Administration
 - System Log
 - WDS
 - Bridge
 - STP
 - RSSI
- RADIO INTERFACE A
 - Radio Settings
 - Security
- RADIO INTERFACE G
 - Radio Settings
 - Security

The main content area is titled "Advanced Setup" and shows the configuration for "802.11a". Under the "Security" section, the "Data Encryption (a) Setup" is set to "Disable". The "Key Type" is set to "Hexadecimal" with a note "Enter 32 digits". Below this, there is a table for configuring keys for different port numbers:

Port Number	Key
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>

Configuring AES encryption keys on the wireless bridge provides far more robust security than using WEP. Also, a unique AES key can be used for each bridge link in the wireless network, instead of all bridges sharing the same WEP keys.

Data Encryption Setup – Enable or disable the wireless bridge to use either WEP or AES for data encryption. If AES encryption is selected and enabled, you must configure one encryption key for each wireless port link on the wireless bridge. A Slave bridge supports only one wireless port link, but a Master bridge supports up to 16 links. (Default: Disable)

Key Type – Select the preferred method of entering AES encryption keys on the wireless bridge and enter a key for each bridge link in the network:

- Hexadecimal: Enter keys as exactly 32 hexadecimal digits (0 to 9 and A to F).
- Alphanumeric: Enter keys as an alphanumeric string using between 8 and 31 characters.

Note: For each wireless port link (1 to 16), the AES keys must match on the corresponding bridge unit.

CLI Commands for WEP Security – From the 802.11a interface configuration mode, use the **encryption** command to enable WEP encryption. To enter WEP keys, use the **key** command, and then set one key as the transmit key using the **transmit-key**

System Configuration

command. To view the current security settings, use the **show interface wireless a** command.

```
AP(config)#interface wireless a                                7-99
Enter Wireless configuration commands, one per line.
AP(if-wireless a)#encryption wep 128                          7-110
AP(if-wireless a)#key wep 1 128 ascii abcdeabcdeabc           7-112
AP(if-wireless a)#transmit-key 1                               7-113
AP(if-wireless a)#exit
AP#show interface wireless a                                    7-120

Wireless Interface Information
=====
-----Identification-----
Description                : Enterprise 802.11a Wireless Outdoor
Bridge/AP
Service Type               : WDS Bridge
SSID                      : DualBandOutdoor
Turbo Mode                 : OFF
Channel                   : 36
Status                    : Disable
-----802.11 Parameters-----
Transmit Power             : FULL (15 dBm)
Max Station Data Rate     : 54Mbps
Fragmentation Threshold   : 2346 bytes
RTS Threshold              : 2347 bytes
Beacon Interval           : 100 TUs
DTIM Interval              : 2 beacons
Maximum Association       : 64 stations
-----Security-----
Encryption                 : 128-BIT WEP ENCRYPTION
WEP Key type               : Alphanumeric
Default Transmit Key       : 1
Static Keys :
    Key 1: *****    Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
=====
AP#
```

Note: The index and length values used in the **key** command must be the same values used in the **encryption** and **transmit-key** commands.

CLI Commands for AES Security – From the 802.11a interface configuration mode, use the **encryption** command to enable AES encryption. To enter AES keys, use the **key** command. To view the current security settings, use the **show interface wireless a** command.

```
AP(config)#interface wireless a                                7-99
Enter Wireless configuration commands, one per line.
AP(if-wireless a)#encryption wdsaes alphanumeric              7-110
AP(if-wireless a)#key wdsaes 1 agoodsecretkey                 7-112
AP(if-wireless a)#exit
AP#show interface wireless a                                   7-120

Wireless Interface Information
=====
-----Identification-----
Description                               : Enterprise 802.11a Wireless Outdoor
Bridge/AP
Service Type                             : WDS Bridge
SSID                                     : DualBandOutdoor
Turbo Mode                               : OFF
Channel                                  : 36
Status                                  : Disable
-----802.11 Parameters-----
Transmit Power                           : FULL (15 dBm)
Max Station Data Rate                     : 54Mbps
Fragmentation Threshold                   : 2346 bytes
RTS Threshold                             : 2347 bytes
Beacon Interval                           : 100 TUs
DTIM Interval                             : 2 beacons
Maximum Association                       : 64 stations
-----Security-----
Encryption                               : 128-BIT AES ENCRYPTION
AES Key type                              : Alphanumeric
=====
AP#
```

Note: The key type value entered using the **key** command must be the same as the type specified in the **encryption** command.

Security (Access Point Mode)

A radio band set to access point mode is configured by default as an “open system,” which broadcasts a beacon signal including the configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the access point.

To improve wireless network security for access point operation, you have to implement two main functions:

- **Authentication:** It must be verified that clients attempting to connect to the network are authorized users.
- **Traffic Encryption:** Data passing between the access point and clients must be protected from interception and eavesdropping.

For a more secure network, the access point can implement one or a combination of the following security mechanisms:

- **Wired Equivalent Privacy (WEP)**page 6-66
- **IEEE 802.1X**page 6-19
- **Wireless MAC address filtering**page 6-19
- **Wi-Fi Protected Access (WPA)**page 6-80

The security mechanisms that may be employed depend on the level of security required, the network and management resources available, and the software support provided on

wireless clients. A summary of wireless security considerations is listed in the following table.

Security Mechanism	Client Support	Implementation Considerations
WEP	Built-in support on all 802.11a and 802.11g devices	<ul style="list-style-type: none">• Provides only weak security• Requires manual key management
WEP over 802.1X	Requires 802.1X client support in system or by add-in software (support provided in Windows 2000 SP3 or later and Windows XP)	<ul style="list-style-type: none">• Provides dynamic key rotation for improved WEP security• Requires configured RADIUS server• 802.1X EAP type may require management of digital certificates for clients and server
MAC Address Filtering	Uses the MAC address of client network card	<ul style="list-style-type: none">• Provides only weak user authentication• Management of authorized MAC addresses• Can be combined with other methods for improved security• Optionally configured RADIUS server
WPA over 802.1X Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	<ul style="list-style-type: none">• Provides robust security in WPA-only mode (i.e., WPA clients only)• Offers support for legacy WEP clients, but with increased security risk (i.e., WEP authentication keys disabled)• Requires configured RADIUS server• 802.1X EAP type may require management of digital certificates for clients and server
WPA PSK Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	<ul style="list-style-type: none">• Provides good security in small networks• Requires manual management of pre-shared key

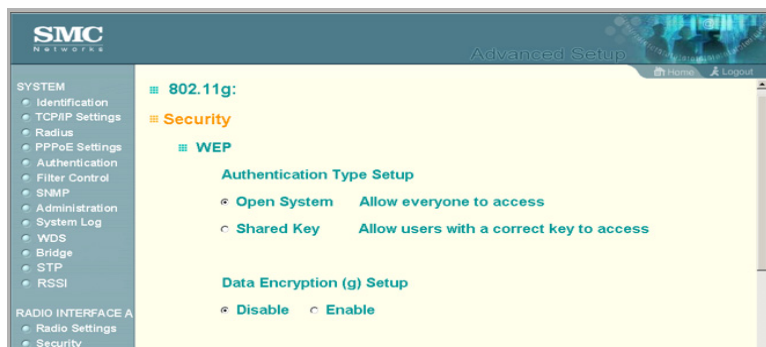
System Configuration

Note: Although a WEP static key is not needed for WEP over 802.1X, WPA over 802.1X, and WPA PSK modes, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point.

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. Unfortunately, WEP has been found to be seriously flawed and cannot be recommended for a high level of network security. For more robust wireless security, the access point provides Wi-Fi Protected Access (WPA) for improved data encryption and user authentication.



Setting up shared keys enables the basic IEEE 802.11 Wired Equivalent Privacy (WEP) on the access point to prevent unauthorized access to the network.

If you choose to use WEP shared keys instead of an open system, be sure to define at least one static WEP key for user

authentication and data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

Authentication Type Setup – Sets the access point to communicate as an open system that accepts network access attempts from any client, or with clients using pre-configured static shared keys.

- **Open System:** Select this option if you plan to use WPA or 802.1X as a security mechanism. If you don't set up any other security mechanism on the access point, the network has no protection and is open to all users. This is the default setting.
- **Shared Key:** Sets the access point to use WEP shared keys. If this option is selected, you must configure at least one key on the access point and all clients.

Note: To use 802.1X on wireless clients requires a network card driver and 802.1X client software that supports the EAP authentication type that you want to use. Windows 2000 SP3 or later and Windows XP provide 802.1X client support. Windows XP also provides native WPA support. Other systems require additional client software to support 802.1X and WPA.

Data Encryption Setup – Enable or disable the access point to use WEP shared keys for data encryption. If this option is selected, you must configure at least one key on the access point and all clients. (Default: Disable)

Note: You must enable data encryption through the web or CLI in order to enable all types of encryption (WEP, TKIP, and AES) in the access point.

System Configuration

SMC Networks Advanced Setup

Home Logout

SYSTEM

- Identification
- TCP/IP Settings
- Radius
- PPPoE Settings
- Authentication
- Filter Control
- SNMP
- Administration
- System Log
- WDS
- Bridge
- STP
- RSSI

RADIO INTERFACE A

- Radio Settings
- Security

RADIO INTERFACE G

- Radio Settings
- Security

Shared Key Setup ☐ 64 Bit ☒ 128 Bit

Key Type ☒ Hexadecimal For 64 Bit enter 10 digits, for 128 Bit enter 26

☐ Alphanumeric For 64 Bit enter 5 characters, for 128 Bit enter 13

Key Number	Transmit Key Select	Key
Key 1	<input checked="" type="radio"/>	<input type="text"/>
Key 2	<input type="radio"/>	<input type="text"/>
Key 3	<input type="radio"/>	<input type="text"/>
Key 4	<input type="radio"/>	<input type="text"/>

Apply Cancel Help

Shared Key Setup – Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. 152 Bit key length is only supported on 802.11a radio. (Default: 128 Bit)

Key Type – Select the preferred method of entering WEP encryption keys on the access point and enter up to four keys:

- **Hexadecimal:** Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys (802.11a radio only).
- **Alphanumeric:** Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys, or 16 alphanumeric characters for 152 bit keys (802.11a radio only).
- **Transmit Key Select:** Selects the key number to use for encryption. If the clients have all four keys configured to the same values, you can change the encryption key to any of the

four settings without having to update the client keys.

Note: Key index and type must match that configured on the clients.

The configuration settings for WEP are summarized below:

WEP only	WEP over 802.1X
Authentication Type: Shared Key	Authentication Type: Open System
WEP (encryption): Enable	WEP (encryption): Enable
WPA clients only: Disable	WPA clients only: Disable
Multicast Cipher: WEP	Multicast Cipher: WEP
Shared Key: 64/128/152	Shared Key: 64/128
Key Type -	802.1X = Required ¹
Hex: 10/26/32 characters	MAC Authentication: Disabled/ Local ²
ASCII: 5/13/16 characters	
Transmit Key: 1/2/3/4 (set index)	
802.1X = Disabled ¹	
MAC Authentication: Any setting ²	

1: See Authentication (page 6-16)

2: See Radius (page 6-10)

CLI Commands for static WEP Shared Key Security – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to enable WEP shared-key authentication and the **encryption** command to enable WEP encryption. Use the **multicast-cipher** command to select WEP cipher type. To enter WEP keys, use the **key** command, and then set one key as the transmit key using the **transmit-key** command. Then disable 802.1X port authentication with the **no 802.1X** command. To view the current security settings, use the

System Configuration

show interface wireless a or **show interface wireless g** command.

```
AP(config)#interface wireless g                                7-99
Enter Wireless configuration commands, one per line.
AP(if-wireless g)#authentication shared                        7-109
AP(if-wireless g)#encryption 128                              7-110
AP(if-wireless g)#multicast-cipher wep                        7-114
AP(if-wireless g)#key 1 128 ascii abcdeabcdeabc               7-112
AP(if-wireless g)#transmit-key 1                              7-113
AP(if-wireless g)#end
AP(config)#no 802.1X                                          7-51
AP(config)#end
AP#show interface wireless g                                  7-120

Wireless Interface Information
=====
-----Identification-----
Description           : Enterprise 802.11g Wlreless Outdoor
Bridge/AP
Service Type          : Access Point
SSID                  : DualBandOutdoor
Channel                : 5 (AUTO)
Status                : Disable
-----802.11 Parameters-----
Transmit Power        : FULL (20 dBm)
Max Station Data Rate : 54Mbps
Fragmentation Threshold : 2346 bytes
RTS Threshold         : 2347 bytes
Beacon Interval       : 100 TUs
DTIM Interval         : 2 beacons
Maximum Association   : 64 stations
-----Security-----
Closed System         : DISABLED
Multicast cipher      : WEP
Unicast cipher        : TKIP
WPA clients           : SUPPORTED
WPA Key Mgmt Mode     : DYNAMIC
WPA PSK Key Type      : HEX
Encryption            : 128-BIT ENCRYPTION
Default Transmit Key  : 1
Static Keys :
    Key 1: *****    Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
Authentication Type   : SHARED
=====
AP#
```

Note: The index and length values used in the **key** command must be the same values used in the **encryption** and **transmit-key** commands.

CLI Commands for WEP over 802.1X Security – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to select open system authentication. Use the **multicast-cipher** command to select WEP cipher type. Then set 802.1X to required with **802.1X** command, and disable MAC authentication with the **mac-authentication** command. To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

AP(config)#interface wireless g	7-99
Enter Wireless configuration commands, one per line.	
AP(if-wireless g)#authentication open	7-109
AP(if-wireless g)#encryption 128	7-110
AP(if-wireless g)#multicast-cipher wep	7-114
AP(if-wireless g)#end	
AP(config)#802.1X required	7-51
AP(config)#no mac-authentication	7-59
AP(config)#	

System Configuration

Wi-Fi Protected Access (WPA)

WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks.

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM, RADIO INTERFACE A, and RADIO INTERFACE G. Under SYSTEM, 'Security' is highlighted. The main content area is titled 'WPA Configuration Mode' and contains several sections: 'WPA Configuration Mode' with radio buttons for 'Supported' (selected), 'WPA clients only', and 'Not Supported'; 'WPA Key Management' with radio buttons for 'WPA authentication over 802.1x' and 'WPA Pre-shared Key' (selected); 'Multicast Cipher Mode' with radio buttons for 'WEP' (selected), 'TKIP', and 'AES', each followed by a description of its use as a WPA Multicast cipher mode; and 'WPA Pre-Shared Key Type' with radio buttons for 'Hexadecimal' (selected) and 'Alphanumeric', each followed by instructions on the number of characters to enter. At the bottom, there is a text input field labeled 'WPA Pre-Shared Key'.

SMC Networks Advanced Setup

SYSTEM

- Identification
- TCR/P Settings
- Radius
- PPPoE Settings
- Authentication
- Filter Control
- SNMP
- Administration
- System Log
- WDS
- Bridge
- STP
- RSSI

RADIO INTERFACE A

- Radio Settings
- Security

RADIO INTERFACE G

- Radio Settings
- Security

WPA Configuration Mode

☒ Supported ☐ WPA clients only ☐ Not Supported

WPA Key Management

☒ WPA authentication over 802.1x

☒ WPA Pre-shared Key

Multicast Cipher Mode

☒ WEP Use WEP as WPA Multicast cipher mode

☐ TKIP Use TKIP as WPA Multicast cipher mode

☐ AES Use AES as WPA Multicast cipher mode

WPA Pre-Shared Key Type

☒ Hexadecimal Enter 64 digits

☐ Alphanumeric Enter between 8 and 63 characters

WPA Pre-Shared Key

The access point supports the following WPA components and features:

IEEE 802.1X and the Extensible Authentication Protocol (EAP):

WPA employs 802.1X as its basic framework for user authentication and dynamic key management. The 802.1X client and RADIUS server should use an appropriate EAP type—such as EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled TLS), or PEAP (Protected EAP)—for strongest authentication. Working together, these protocols provide “mutual authentication” between a client, the access point, and a RADIUS server that prevents users from accidentally joining a rogue network. Only

when a RADIUS server has authenticated a user's credentials will encryption keys be sent to the access point and client.

Note: To implement WPA on wireless clients requires a WPA-enabled network card driver and 802.1X client software that supports the EAP authentication type that you want to use. Windows XP provides native WPA support, other systems require additional software.

Temporal Key Integrity Protocol (TKIP): WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys. Basically, TKIP starts with a master (temporal) key for each user session and then mathematically generates other keys to encrypt each data packet. TKIP provides further data encryption enhancements by including a message integrity check for each packet and a re-keying mechanism, which periodically changes the master key.

WPA Pre-Shared Key (PSK) Mode: For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.

Mixed WPA and WEP Client Support: WPA enables the access point to indicate its supported encryption and authentication mechanisms to clients using its beacon signal. WPA-compatible clients can likewise respond to indicate their WPA support. This enables the access point to determine which clients are using WPA security and which are using legacy WEP. The access point

System Configuration

uses TKIP unicast data encryption keys for WPA clients and WEP unicast keys for WEP clients. The global encryption key for multicast and broadcast traffic must be the same for all clients, therefore it restricts encryption to a WEP key.

When access is opened to both WPA and WEP clients, no authentication is provided for the WEP clients through shared keys. To support authentication for WEP clients in this mixed mode configuration, you can use either MAC authentication or 802.1X authentication.

Advanced Encryption Standard (AES) Support: WPA specifies AES encryption as an optional alternative to TKIP and WEP. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP. The developing IEEE 802.11i wireless security standard has specified AES as an eventual replacement for TKIP and WEP. However, because of the difference in ciphering algorithms, AES requires new hardware support in client network cards that is currently not widely available. The access point includes AES support as a future security enhancement.

The WPA configuration parameters are described below:

Authentication Type Setup – When using WPA, set the access point to communicate as an open system to disable WEP keys.

Note: Although WEP keys are not needed for WPA, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point. For example, set Wired Equivalent Privacy (WEP) Setup to “Enable” on the Security page.

WPA Configuration Mode – The access point can be configured to allow only WPA-enabled clients to access the network, or also allow clients only capable of supporting WEP.

WPA Key Management – WPA can be configured to work in an enterprise environment using IEEE 802.1X and a RADIUS server for user authentication. For smaller networks, WPA can be enabled using a common pre-shared key for client authentication with the access point.

- **WPA authentication over 802.1X:** The WPA enterprise mode that uses IEEE 802.1X to authenticate users and to dynamically distribute encryption keys to clients.
- **WPA Pre-shared Key:** The WPA mode for small networks that uses a common password string that is manually distributed. If this mode is selected, be sure to also specify the key string.

Multicast Cipher Mode – Selects an encryption method for the global key used for multicast and broadcast traffic, which is supported by all wireless clients.

- **WEP:** WEP is the first generation security protocol used to encrypt data crossing the wireless medium using a fairly short key. Communicating devices must use the same WEP key to encrypt and decrypt radio signals. WEP has many security flaws, and is not recommended for transmitting highly-sensitive data.

System Configuration

- **TKIP:** TKIP provides data encryption enhancements including per-packet key hashing (that is, changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.
- **AES:** AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 standard.

WPA Pre-Shared Key Type – If the WPA pre-shared-key mode is used, all wireless clients must be configured with the same key to communicate with the access point.

- **Hexadecimal:** Enter a key as a string of 64 hexadecimal numbers.
- **Alphanumeric:** Enter a key as an easy-to-remember form of letters and numbers. The string must be from 8 to 63 characters, which can include spaces.

The configuration settings for WPA are summarized below:

WPA pre-shared key only	WPA over 802.1X
Authentication Type: Open System	Authentication Type: Open System
WEP (encryption): Enable ¹	WEP (encryption): Enable ¹
WPA clients only: Enable	WPA clients only: Enable
WPA Mode: Pre-shared-key	WPA Mode: WPA over 802.1X
Multicast Cipher: WEP/TKIP/AES ²	Multicast Cipher: WEP/TKIP/AES ²
WPA PSK Type -	Shared Key: 64/128/152
Hex: 64 characters	802.1X = Required ³
ASCII: 8-63 characters	MAC Authentication: Disabled/ Local ⁴
Shared Key: 64/128/152	
802.1X = Disabled ³	
MAC Authentication: Disabled/ Local ⁴	

- 1: Although WEP keys are not needed for WPA, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point. For example, use the CLI **encryption** command to set Encryption = 64, 128 or 152, thus enabling encryption (i.e., all types of encryption) in the access point.
- 2: Do not use WEP unless the access point must support both WPA and WEP clients.
- 3: See Authentication (page 6-16)
- 4: See Radius (page 6-10)

CLI Commands for WPA Pre-shared Key Security – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to set the access point to “Open System.” Use the WEP **encryption** command to enable all types of encryption. To enable WPA to be required for all clients, use the **wpa-clients** command. Use the **wpa-mode** command to enable the Pre-shared Key mode. To enter a key value, use the **wpa-psk-type** command to specify a hexadecimal or alphanumeric key, and then use the **wpa-preshared-key** command to define the key. Then disable 802.1X and MAC

System Configuration

authentication. To view the current 802.11g security settings, use the **show interface wireless a** or **show interface wireless g** command (not shown in example).

AP(config)#interface wireless g	7-99
Enter Wireless configuration commands, one per line.	
AP(if-wireless g)#authentication open	7-109
AP(if-wireless g)#encryption 128	7-110
AP(if-wireless g)#wpa-clients required	7-116
AP(if-wireless g)#wpa-mode pre-shared-key	7-117
AP(if-wireless g)#wpa-psk-type alphanumeric	7-119
AP(if-wireless g)#wpa-preshared-key ASCII asecret	7-118
AP(if-wireless g)#end	
AP(config)#no 802.1X	7-51
AP(config)#no mac-authentication	7-59

CLI Commands for WPA over 802.1X Security – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to set the access point to “Open System.” Use the WEP **encryption** command to enable all types of encryption. Use the **wpa-clients** command to set WPA to be required or supported for clients. Use the **wpa-mode** command to enable WPA dynamic keys over 802.1X. Set the broadcast and multicast key encryption using the **multicast-cipher** command. Then set 802.1X to required, and disable MAC authentication. To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

AP(config)#interface wireless g	7-99
Enter Wireless configuration commands, one per line.	
AP(if-wireless g)#authentication open	7-109
AP(if-wireless g)#encryption 128	7-110
AP(if-wireless g)#wpa-clients required	7-116
AP(if-wireless g)#wpa-mode dynamic	7-117
AP(if-wireless g)#multicast-cipher TKIP	7-114
AP(if-wireless g)#end	
AP(config)#802.required	7-51
AP(config)#no mac-authentication	7-59

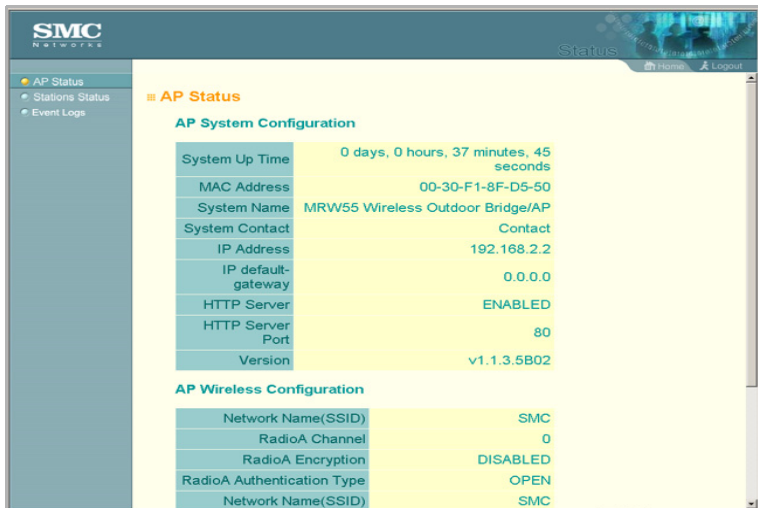
Status Information

The Status page includes information on the following items:

Menu	Description	Page
AP Status	Displays configuration settings for the basic system and the wireless interfaces	6-87
Station Status	Shows wireless clients currently associated with the access point	6-90
Event Logs	Shows log messages stored in memory	6-92

AP Status

The AP Status window displays basic system configuration settings, as well as the settings for the wireless interfaces.



AP System Configuration	
System Up Time	0 days, 0 hours, 37 minutes, 45 seconds
MAC Address	00-30-F1-8F-D5-50
System Name	MRW55 Wireless Outdoor Bridge/AP
System Contact	Contact
IP Address	192.168.2.2
IP default-gateway	0.0.0.0
HTTP Server	ENABLED
HTTP Server Port	80
Version	v1.1.3.5B02

AP Wireless Configuration	
Network Name(SSID)	SMC
RadioA Channel	0
RadioA Encryption	DISABLED
RadioA Authentication Type	OPEN
Network Name(SSID)	SMC

AP System Configuration – The AP System Configuration table displays the basic system configuration settings:

System Configuration

- **System Up Time:** Length of time the management agent has been up.
- **MAC Address:** The physical layer address for this device.
- **System Name:** Name assigned to this system.
- **System Contact:** Administrator responsible for the system.
- **IP Address:** IP address of the management interface for this device.
- **IP Default Gateway:** IP address of the gateway router between this device and management stations that exist on other network segments.
- **HTTP Server:** Shows if management access via HTTP is enabled.
- **HTTP Server Port:** Shows the TCP port used by the HTTP interface.
- **Version:** Shows the version number for the runtime code.

AP Wireless Configuration – The AP Wireless Configuration table displays the wireless interface settings listed below. Note that Radio A refers to the 802.11a interface and Radio G to the 802.11b/g interface.

- **Network Name (SSID):** The service set identifier for this wireless group.
- **Radio Channel:** The radio channel currently used on the wireless bridge.
- **Radio Encryption:** The key size used for data encryption.

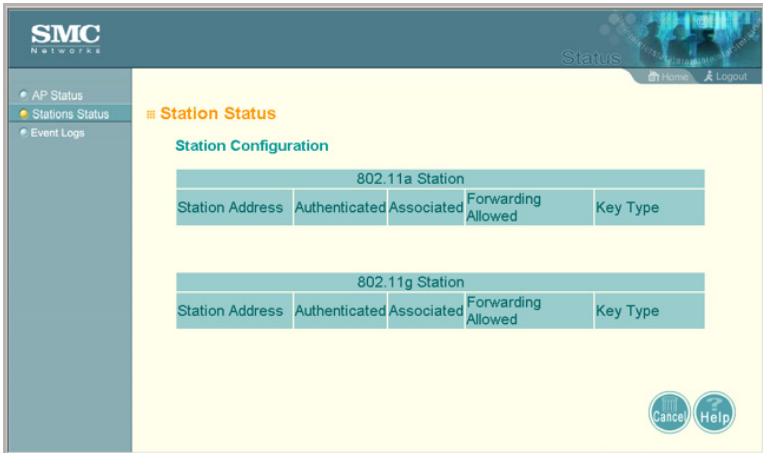
- Radio Authentication Type: Shows the bridge is set as an open system.
- 802.1X: Shows if IEEE 802.1X access control for wireless clients is enabled.

CLI Commands for Displaying System Settings – To view the current wireless bridge system settings, use the **show system** command from the Exec mode. To view the current radio interface settings, use the **show interface wireless a** command (see page 7-120).

```
AP#show system 7-22
System Information
=====
Serial Number      : .
System Up time     : 0 days, 5 hours, 2 minutes, 4 seconds
System Name        : Dual Band Outdoor AP
System Location    :
System Contact     : Contact
System Country Code : US - UNITED STATES
MAC Address        : 00-03-7F-BE-F8-99
IP Address         : 192.168.2.2
Subnet Mask        : 255.255.255.0
Default Gateway    : 0.0.0.0
VLAN State         : DISABLED
Native VLAN ID     : 1
IAPP State         : ENABLED
DHCP Client        : ENABLED
HTTP Server        : ENABLED
HTTP Server Port   : 80
Slot Status        : Dual band(a/g)
Software Version    : v1.1.0.0B07
=====
AP#
```

Station Status

The Station Status window shows wireless clients currently associated with the access point.



The Station Status page displays basic connection information for all associated stations. Note that this page is automatically refreshed every five seconds.

- **Station Address:** The MAC address of the remote wireless bridge.
- **Authenticated:** Shows if the station has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to stations before attempting authentication.

- **Associated:** Shows if the station has been successfully associated with the access point.
- **Forwarding Allowed:** Shows if the station has passed authentication and is now allowed to forward traffic.
- **Key Type:** Displays one of the following:
 - **Disabled:** The client is not using Wired Equivalent Privacy (WEP) encryption keys.
 - **Dynamic:** The client is using Wi-Fi Protected Access (802.1X or pre-shared key mode) or using 802.1X authentication with dynamic keying.
 - **Static:** The client is using static WEP keys for encryption.

CLI Commands for Displaying Station Information – To view status of clients currently associated with the access point, use the **show station** command from the Exec mode.

```
AP#show station 7-121

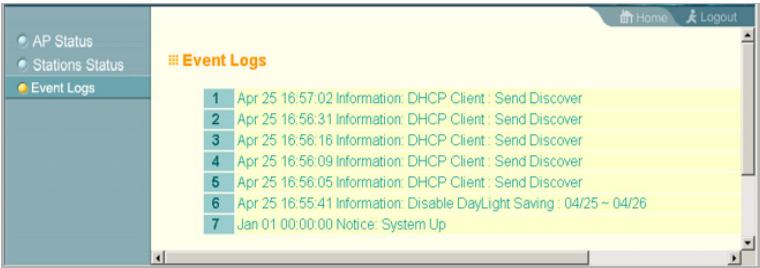
Station Table Information
=====
802.11a Channel : 56

No 802.11a Channel Stations.
802.11g Channel : 11
802.11g Channel Station Table
Station Address   : 00-04-E2-41-C2-9D VLAN ID: 0
Authenticated Associated Forwarding KeyType
TRUE             TRUE     TRUE     NONE
Counters:pkts    Tx      /    Rx    bytes  Tx      /    Rx
                  4/      0      1440/   0
Time:Associated  LastAssoc LastDisAssoc LastAuth
      143854      0          0          0
=====
AP#
```

System Configuration

Event Logs

The Event Logs window shows the log messages generated by the wireless bridge and stored in memory.



The Event Logs table displays the following information:

- Log Time: The time the log message was generated.
- Event Level: The logging level associated with this message. For a description of the various levels, see “logging level” on page 6-38.
- Event Message: The content of the log message.

CLI Commands for Displaying the Event Logs – From the global configuration mode, use the **show logging** command.

```
AP#show logging 7-27

Logging Information
=====
Syslog State           : Enabled
Logging Host State     : Enabled
Logging Console State  : Enabled
Server Domain name/IP : 192.168.1.19
Logging Level          : Alert
Logging Facility Type   : 16
=====

AP#
```


System Configuration

Chapter 7

Command Line Interface

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the wireless bridge via a Telnet connection, the wireless bridge can be managed by entering command keywords and parameters at the prompt. Using the wireless bridge's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, if the wireless bridge cannot acquire an IP address from a DHCP server, the default IP address used by the wireless bridge, 192.168.2.2, consists of a network portion (192.168.2) and a host portion (2).

To access the wireless bridge through a Telnet session, you must first set the IP address for the wireless bridge, and set the default

Command Line Interface

gateway if you are managing the wireless bridge from a different IP subnet. For example:

```
AP#configure
AP(config)#interface ethernet
AP(if-ethernet)#ip address 10.1.0.1 255.255.255.0
    10.1.0.254
AP(if-ethernet)#
```

After you configure the wireless bridge with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “AP#” prompt to show that you are using executive access mode (i.e., Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:
AP#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interface ethernet,” **show** and **interface** are keywords, and **ethernet** is an argument that specifies the interface type.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
AP(config)#username smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “configure” example, typing **con** followed by a tab will result in printing the command up to “**configure**.”

Command Line Interface

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by following a command with the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current configuration mode (Exec, Global Configuration, or Interface). You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Outdoor Bridge#show ?
 authentication      Show Authentication parameters
 bootfile             Show bootfile name
 bridge              Show bridge table
 filters              Show filters
 hardware             Show hardware version
 history              Display the session history
 interface            Show interface information
 line                 TTY line information
 logging              Show the logging buffers
 memory-allocation    Show memory allocation
 pppoe                Show PPPoE parameters
 radius               Show radius server
 snmp                 Show snmp statistics
 sntp                 Show sntp statistics
 station              Show 802.11 station table
 system               Show system information
 version              Show system version
 wds                  Show wds table
DUAL OUTDOOR#showAP#show ?
```

The command “**show interface ?**” will display the following information:

```
AP#show interface ?
  ethernet  Show Ethernet interface
  wireless  Show wireless interface
  <cr>
AP#show interface
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
AP#show s?
snmp      sntp      station  system
AP#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “?” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	Mode
Exec	Privileged
Configuration	Global Interface-ethernet Interface-wireless

Exec Commands

When you open a new console session on wireless bridge, the system enters Exec command mode. Only a limited number of the commands are available in this mode. You can access all other commands only from the configuration mode. To access Exec mode, open a new console session with the user name “admin.” The command prompt displays as “AP#” for Exec mode.

```
Username: admin
Password: [system login password]
AP#
```


Configuration Commands

Configuration commands are used to modify wireless bridge settings. These commands modify the running configuration and are saved in memory.

The configuration commands are organized into three different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **username** and **password**.
- Interface-Ethernet Configuration - These commands modify the Ethernet port configuration, and include command such as **dns** and **ip**.
- Interface-Wireless Configuration - These commands modify the wireless port configuration, and include command such as **channel** and **encryption**.

To enter the Global Configuration mode, enter the command **configure** in Exec mode. The system prompt will change to “AP(config)#” which gives you access privilege to all Global Configuration commands.

```
AP#configure
AP(config)#
```

To enter Interface mode, you must enter the “**interface ethernet**” or “**interface wireless a**” command while in Global Configuration mode. The system prompt will change to “AP(if-ethernet)#,” or “AP(if-wireless a)” indicating that you have access privileges to the associated commands. You can use the **end** command to return to the Exec mode.

```
AP(config)#interface ethernet
AP(if-ethernet)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates a task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes from cursor to the end of the command line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Shows the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor backward one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description	Page
General	Basic commands for entering configuration mode, restarting the system, or quitting the CLI	7-10
System Management	Controls user name, password, browser management options, and a variety of other system information	7-15
System Logging	Configures system logging parameters	7-23
System Clock	Configures SNTP and system clock settings	7-28
SNMP	Configures community access strings and trap managers	7-34
Flash/File	Manages code image or wireless bridge configuration files	7-39
RADIUS	Configures the RADIUS client used with 802.1x authentication	7-45
Authentication	Configures IEEE 802.1x port access control and address filtering	7-49
WDS	Configures the Wireless Distribution System forwarding table	7-61
Bridge	Configures MAC address table aging time settings and spanning tree parameters	7-65
Filtering	Filters access to the management interface from wireless nodes, and filters traffic using specific Ethernet protocol types	7-76
PPPoE	Configures parameters for a PPPoE management tunnel on the Ethernet interface	7-80
Ethernet Interface	Configures connection parameters for the Ethernet interface	7-91
Wireless Interface	Configures connection parameters for the wireless interface	7-97

Command Line Interface

Command Group	Description	Page
IAPP	Enables roaming between multi-vendor access points	7-122
VLANs	Configures VLAN support	7-123

The access mode shown in the following tables is indicated by these abbreviations: **GC** (Global Configuration), **IC-E** (Ethernet Interface Configuration), and **IC-W** (Wireless Interface Configuration).

General Commands

Command	Function	Mode	Page
configure	Activates global configuration mode	Exec	7-10
end	Returns to the previous configuration mode	GC, IC	7-11
exit	Returns to Exec mode, or exits the CLI	any	7-11
ping	Sends ICMP echo request packets to another node on the network	Exec	7-12
reset	Restarts the system	Exec	7-13
show history	Shows the command history buffer	Exec	7-14
show line	Shows the configuration settings for the console port	Exec	7-14

configure

This command activates Global Configuration mode. You must enter this mode to modify most of the settings on the wireless bridge. You must also enter Global Configuration mode prior to enabling the context modes for Interface Configuration. see “Using the Command Line Interface” on page 7-1

Default Setting

None

Command Mode

Exec

Example

```
AP#configure
AP(config)#
```

Related Commands

end (page 7-11)

end

This command returns to the previous configuration mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration

Example

This example shows how to return to the Configuration mode from the Interface Configuration mode:

```
AP(if-ethernet)#end
AP(config)#
```

exit

This command returns to the Exec mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Command Line Interface

Example

This example shows how to return to the Exec mode from the Interface Configuration mode, and then quit the CLI session:

```
AP(if-ethernet)#exit
AP#exit
CLI session with the wireless bridge is now closed

Username:
```

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping <host_name / ip_address>

- *host_name* - Alias of the host.
- *ip_address* - IP address of the host.

Default Setting

None

Command Mode

Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
 - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.

- *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
AP#ping 10.1.0.19
192.168.1.19 is alive
AP#
```

reset

This command restarts the system or restores the factory default settings.

Syntax

reset <board | configuration>

- **board** - Reboots the system.
- **configuration** - Resets the configuration settings to the factory defaults, and then reboots the system.

Default Setting

None

Command Mode

Exec

Command Usage

When the system is restarted, it will always run the Power-On Self-Test.

Example

This example shows how to reset the system:

```
AP#reset board
Reboot system now? <y/n>: y
```

Command Line Interface

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Exec

Command Usage

- The history buffer size is fixed at 10 commands.
- Use the up or down arrow keys to scroll through the commands in the history buffer.

Example

In this example, the show history command lists the contents of the command history buffer:

```
AP#show history
  config
  exit
  show history
AP#
```

show line

This command displays the console port's configuration settings.

Command Mode

Exec

System Management Commands

Example

The console port settings are fixed at the values shown below.

```
AP#show line
Console Line Information
=====
databits   : 8
parity     : none
speed      : 9600
stop bits  : 1
=====
AP#
```

System Management Commands

These commands are used to configure the user name, password, browser management options, and a variety of other system information.

Command	Function	Mode	Page
<i>Country Setting</i>			
country	Sets the wireless bridge country code for correct radio operation	Exec	7-16
<i>Device Designation</i>			
prompt	Customizes the command line prompt	GC	7-18
system name	Specifies the host name for the wireless bridge	GC	7-19
snmp-server contact	Sets the system contact string	GC	7-35
snmp-server location	Sets the system location string	GC	7-38
<i>User Access</i>			
username	Configures the user name for management access	GC	7-19
password	Specifies the password for management access	GC	7-20

Command Line Interface

Command	Function	Mode	Page
<i>Web Server</i>			
ip http port	Specifies the port to be used by the web browser interface	GC	7-20
ip http server	Allows the wireless bridge to be monitored or configured from a browser	GC	7-21
<i>System Status</i>			
show system	Displays system information	Exec	7-22
show version	Displays version information for the system	Exec	7-23

country

This command configures the wireless bridge's country code, which identifies the country of operation and sets the authorized radio channels.

Syntax

country <country_code>

country_code - A two character code that identifies the country of operation. See the following table for a full list of codes.

Country	Code	Country	Code	Country	Code	Country	Code
Albania	AL	Dominican Republic	DO	Kuwait	KW	Romania	RO
Algeria	DZ	Ecuador	EC	Latvia	LV	Russia	RU
Argentina	AR	Egypt	EG	Lebanon	LB	Saudi Arabia	SA
Armenia	AM	Estonia	EE	Liechtenstein	LI	Singapore	SG
Australia	AU	Finland	FI	Lithuania	LT	Slovak Republic	SK
Austria	AT	France	FR	Luxembourg	LU	Slovenia	SI
Azerbaijan	AZ	Georgia	GE	Macao	MO	South Africa	ZA
Bahrain	BH	Germany	DE	Macedonia	MK	Spain	ES
Belarus	BY	Greece	GR	Malaysia	MY	Sweden	SE
Belgium	BE	Guatemala	GT	Mexico	MX	Switzerland	CH

System Management Commands

Country	Code	Country	Code	Country	Code	Country	Code
Belize	BZ	Hong Kong	HK	Monaco	MC	Syria	SY
Bolivia	BO	Hungary	HU	Morocco	MA	Taiwan	TW
Brazil	BR	Iceland	IS	Netherlands	NL	Thailand	TH
Brunei Darussalam	BN	India	IN	New Zealand	NZ	Turkey	TR
Bulgaria	BG	Indonesia	ID	Norway	NO	Ukraine	UA
Canada	CA	Iran	IR	Oman	OM	United Arab Emirates	AE
Chile	CL	Ireland	IE	Pakistan	PK	United Kingdom	GB
China	CN	Israel	IL	Panama	PA	United States	US
Colombia	CO	Italy	IT	Peru	PE	Uruguay	UY
Costa Rica	CR	Japan	JP	Philippines	PH	Venezuela	VE
Croatia	HR	Jordan	JO	Poland	PL	Vietnam	VN
Cyprus	CY	Kazakhstan	KZ	Portugal	PT		
Czech Republic	CZ	North Korea	KP	Puerto Rico	PR		
Denmark	DK	Korea Republic	KR	Qatar	QA		

Default Setting

US - for units sold in the United States

99 (no country set) - for units sold in other countries

Command Mode

Exec

Command Usage

- If you purchased an wireless bridge outside of the United States, the country code must be set before radio functions are enabled.
- The available Country Code settings can be displayed by using the **country ?** command.

Command Line Interface

Example

```
AP#country us
AP#
```

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*

no prompt

string - Any alphanumeric string to use for the CLI prompt.
(Maximum length: 255 characters)

Default Setting

Dual Outdoor

Command Mode

Global Configuration

Example

```
AP(config)#prompt RD2
RD2(config)#
```

system name

This command specifies or modifies the system name for this device. Use the **no** form to restore the default system name.

Syntax

system name *name*

no system name

name - The name of this host.

(Maximum length: 32 characters)

Default Setting

Outdoor Bridge

Command Mode

Global Configuration

Example

```
AP(config)#system name bridge-link
AP(config)#
```

username

This command configures the user name for management access.

Syntax

username *name*

name - The name of the user.

(Length: 3-16 characters, case sensitive)

Default Setting

admin

Command Mode

Global Configuration

Command Line Interface

Example

```
AP(config)#username bob
AP(config)#
```

password

After initially logging onto the system, you should set the password. Remember to record it in a safe place. Use the **no** form to reset the default password.

Syntax

password *password*
no password

password - Password for management access.
(Length: 3-16 characters, case sensitive)

Default Setting

smcadmin

Command Mode

Global Configuration

Example

```
AP(config)#password bridgelink
AP(config)#
```

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1024-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
AP(config)#ip http port 1143
AP(config)#
```

Related Commands

ip http server (page 7-21)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
AP(config)#ip http server
AP(config)#
```

Related Commands

ip http port (page 7-20)

Command Line Interface

show system

This command displays basic system configuration settings.

Default Setting

None

Command Mode

Exec

Example

```
AP#show system
System Information
=====
Serial Number       : 0000000000
System Up time      : 0 days, 0 hours, 17 minutes, 2
                      seconds
System Name         : Dual Band Outdoor AP
System Location     :
System Contact      : Contact
System Country Code : TW - TAIWAN
MAC Address         : 00-03-7F-E0-06-EA
IP Address          : 192.168.2.2
Subnet Mask         : 255.255.255.0
Default Gateway     : 0.0.0.0
VLAN State          : DISABLED
Native VLAN ID      : 1
IAPP State          : ENABLED
DHCP Client         : ENABLED
HTTP Server         : ENABLED
HTTP Server Port    : 80
Slot Status         : Dual band(a/g)
Software Version    : v1.1.2.1B05
=====
AP#
```


show version

This command displays the software version for the system.

Default Setting

None

Command Mode

Exec

Example

```
AP#show version
Version v1.1.2.1B05
AP#
```

System Logging Commands

These commands are used to configure system logging on the wireless bridge.

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	7-24
logging host	Adds a syslog server host IP address that will receive logging messages	GC	7-24
logging console	Initiates logging of error messages to the console	GC	7-25
logging level	Defines the minimum severity level for event logging	GC	7-25
logging facility-type	Sets the facility type for remote logging of syslog messages	GC	7-26
show logging	Displays the state of logging	Exec	7-27

Command Line Interface

logging on

This command controls logging of error messages; i.e., sending debug or error messages to memory. The **no** form disables the logging process.

Syntax

logging on
no logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to memory. You can use the **logging level** command to control the type of error messages that are stored in memory.

Example

```
AP(config)#logging on
AP(config)#
```

logging host

This command specifies a syslog server host that will receive logging messages. Use the **no** form to remove syslog server host.

Syntax

logging host <*host_name* | *host_ip_address*>
no logging host

- *host_name* - The name of a syslog server.
(Range: 1-20 characters)
- *host_ip_address* - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Example

```
AP(config)#logging host 10.1.0.3
AP(config)#
```

logging console

This command initiates logging of error messages to the console. Use the **no** form to disable logging to the console.

Syntax

logging console
no logging console

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
AP(config)#logging console
AP(config)#
```

logging level

This command sets the minimum severity level for event logging.

Syntax

logging level <Emergency | Alert | Critical | Error | Warning
| Notice | Informational | Debug>

Command Line Interface

Default Setting

Error

Command Mode

Global Configuration

Command Usage

Messages sent include the selected level down to the Emergency level.

Level Argument	Description
Emergency	System unusable
Alert	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

Example

```
AP(config)#logging level alert
AP(config)#
```

logging facility-type

This command sets the facility type for remote logging of syslog messages.

Syntax

logging facility-type <type>

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service.
(Range: 16-23)

Default Setting

16

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the wireless bridge. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
AP(config)#logging facility 19
AP(config)#
```

show logging

This command displays the logging configuration.

Syntax

show logging

Command Mode

Exec

Command Line Interface

Example

```
AP#show logging

Logging Information
=====
Syslog State           : Disabled
Logging Host State     : Enabled
Logging Console State  : Disabled
Server Domain name/IP : none
Logging Level          : Error
Logging Facility Type  : 16
=====

AP#
```

System Clock Commands

These commands are used to configure SNTP and system clock settings on the wireless bridge.

Command	Function	Mode	Page
sntp-server ip	Specifies one or more time servers	GC	7-29
sntp-server enable	Accepts time from the specified time servers	GC	7-30
sntp-server date-time	Manually sets the system date and time	GC	7-31
sntp-server daylight-saving	Sets the start and end dates for daylight savings time	GC	7-31
sntp-server timezone	Sets the time zone for the wireless bridge's internal clock	GC	7-32
show sntp	Shows current SNTP configuration settings	Exec	7-33

sntp-server ip

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp-server ip <1 | 2> <ip>

- **1** - First time server.
- **2** - Second time server.
- *ip* - IP address of an time server (NTP or SNTP).

Default Setting

137.92.140.80

192.43.244.18

Command Mode

Global Configuration

Command Usage

When SNTP client mode is enabled using the **sntp-server enable** command, the **sntp-server ip** command specifies the time servers from which the wireless bridge polls for time updates. The wireless bridge will poll the time servers in the order specified until a response is received.

Example

```
AP(config)#sntp-server ip 10.1.0.19
AP#
```

Related Commands

sntp-server enable (page 7-30)

show sntp (page 7-33)

sntp-server enable

This command enables SNTP client requests for time synchronization with NTP or SNTP time servers specified by the **sntp-server ip** command. Use the **no** form to disable SNTP client requests.

Syntax

sntp-server enable
no sntp-server enable

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the wireless bridge only records the time starting from the factory default set at the last bootup (i.e., 00:14:00, January 1, 1970).

Example

```
AP(config)#sntp-server enable
AP(config)#
```

Related Commands

sntp-server ip (page 7-29)
show sntp (page 7-33)

sntp-server date-time

This command sets the system clock.

Default Setting

00:14:00, January 1, 1970

Command Mode

Global Configuration

Example

This example sets the system clock to 17:37 June 19, 2003.

```
AP#sntp-server date-time
Enter Year<1970-2100>: 2003
Enter Month<1-12>: 6
Enter Day<1-31>: 19
Enter Hour<0-23>: 17
Enter Min<0-59>: 37
AP#
```

Related Commands

sntp-server enable (page 7-30)

sntp-server daylight-saving

This command sets the start and end dates for daylight savings time. Use the **no** form to disable daylight savings time.

Syntax

sntp-server daylight-saving
no sntp-server daylight-saving

Default Setting

Disabled

Command Mode

Global Configuration

Command Line Interface

Command Usage

The command sets the system clock back one hour during the specified period.

Example

This sets daylight savings time to be used from July 1st to September 1st.

```
AP(config)#sntp-server daylight-saving
Enter Daylight saving from which month<1-12>: 6
and which day<1-31>: 1
Enter Daylight saving end to which month<1-12>: 9
and which day<1-31>: 1
AP(config)#
```

sntp-server timezone

This command sets the time zone for the wireless bridge's internal clock.

Syntax

sntp-server timezone <hours>

hours - Number of hours before/after UTC.
(Range: -12 to +12 hours)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero

degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
AP(config)#ntp-server timezone +8
AP(config)#
```

show ntp

This command displays the current time and configuration settings for the SNTP client.

Command Mode

Exec

Example

```
AP#show ntp

SNTP Information
=====
Service State      : Enabled
SNTP (server 1) IP : 137.92.140.80
SNTP (server 2) IP : 192.43.244.18
Current Time       : 08 : 04, Jun 20th, 2003
Time Zone          : +8 (TAIPEI, BEIJING)
Daylight Saving    : Enabled, from Jun, 1st to Sep, 1st
=====

AP#
```

SNMP Commands

Controls access to this wireless bridge from management stations using the Simple Network Management Protocol (SNMP), as well as the hosts that will receive trap messages.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	7-34
snmp-server contact	Sets the system contact string	GC	7-35
snmp-server enable server	Enables SNMP service and traps	GC	7-36
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	7-37
snmp-server location	Sets the system location string	GC	7-38
show snmp	Displays the status of SNMP communications	Exec	7-39

snmp-server community

This command defines the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro** | **rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 23 characters, case sensitive)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- **public** - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

If you enter a community string without the **ro** or **rw** option, the default is read only.

Example

```
AP(config)#snmp-server community alpha rw
AP(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact.
(Maximum length: 255 characters)

Default Setting

Contact

Command Mode

Global Configuration

Command Line Interface

Example

```
AP(config)#snmp-server contact Paul
AP(config)#
```

Related Commands

snmp-server location (page 7-38)

snmp-server enable server

This command enables SNMP management access and also enables this device to send SNMP traps (i.e., notifications). Use the **no** form to disable SNMP service and trap messages.

Syntax

snmp-server enable server
no snmp-server enable server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This command enables both authentication failure notifications and link-up-down notifications.
- The **snmp-server host** command specifies the host device that will receive SNMP notifications.

Example

```
AP(config)#snmp-server enable server
AP(config)#
```

Related Commands

snmp-server host (page 7-37)

snmp-server host

This command specifies the recipient of an SNMP notification. Use the **no** form to remove the specified host.

Syntax

snmp-server host <*host_ip_address* | *host_name*>
<*community-string*>

no snmp-server host

- *host_ip_address* - IP of the host (the targeted recipient).
- *host_name* - Name of the host. (Range: 1-20 characters)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 23 characters)

Default Setting

Host Address: None

Community String: public

Command Mode

Global Configuration

Command Usage

The **snmp-server host** command is used in conjunction with the **snmp-server enable server** command to enable SNMP notifications.

Command Line Interface

Example

```
AP(config)#snmp-server host 10.1.19.23 batman
AP(config)#
```

Related Commands

snmp-server enable server (page 7-36)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
AP(config)#snmp-server location building-1
AP(config)#
```

Related Commands

snmp-server contact (page 7-35)

show snmp

This command displays the SNMP configuration settings.

Command Mode

Exec

Example

```
AP#show snmp

SNMP Information
=====
Service State   : Enable
Community (ro)  : *****
Community (rw)  : *****
Location        : WC-19
Contact         : Paul
Traps           : Enabled
Host Name/IP    : 10.1.19.23
Trap Community  : *****
=====

AP#
```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode	Page
bootfile	Specifies the file or image used to start up the system	Exec	7-40
copy	Copies a code image or configuration between flash memory and a FTP/TFTP server	Exec	7-41
delete	Deletes a file or code image	Exec	7-42
dir	Displays a list of files in flash memory	Exec	7-43

Command Line Interface

bootfile

This command specifies the image used to start up the system.

Syntax

bootfile <filename>

filename - Name of the image file.

Default Setting

None

Command Mode

Exec

Command Usage

- The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- If the file contains an error, it cannot be set as the default file.

Example

```
AP#bootfile bridge-img.bin
AP#
```

copy

This command copies a boot file, code image, or configuration file between the wireless bridge's flash memory and a FTP/TFTP server. When you save the configuration settings to a file on a FTP/TFTP server, that file can later be downloaded to the wireless bridge to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

Syntax

copy <ftp | tftp> file
copy config <ftp | tftp>

- **ftp** - Keyword that allows you to copy to/from an FTP server.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **file** - Keyword that allows you to copy to/from a flash memory file.
- **config** - Keyword that allows you to upload the configuration file from flash memory.

Default Setting

None

Command Mode

Exec

Command Usage

- The system prompts for data required to complete the copy command.
- Only a configuration file can be uploaded to an FTP/TFTP server, but every type of file can be downloaded to the wireless bridge.

Command Line Interface

- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the wireless bridge. (Valid characters: A-Z, a-z, 0-9, ".", ",", "_")
- Due to the size limit of the flash memory, the wireless bridge supports only two operation code files.
- The system configuration file must be named "syscfg" in all copy commands.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
AP#copy config tftp
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
AP#
```

The following example shows how to download a configuration file:

```
AP#copy tftp file
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:2
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
AP#
```

delete

This command deletes a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Exec

Caution: Beware of deleting application images from flash memory. At least one application image is required in order to boot the wireless bridge. If there are multiple image files in flash memory, and the one used to boot the wireless bridge is deleted, be sure you first use the **bootfile** command to update the application image file booted at startup before you reboot the wireless bridge.

Example

This example shows how to delete the test.cfg configuration file from flash memory.

```
AP#delete test.cfg
Are you sure you wish to delete this file? <y/n>:
AP#
```

Related Commands

bootfile (page 7-40)

dir (page 7-43)

dir

This command displays a list of files in flash memory.

Command Mode

Exec

Command Line Interface

Command Usage

File information is shown below:

Column Heading	Description
File Name	The name of the file.
Type	(2) Operation Code and (5) Configuration file
File Size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
AP#dir

    apimg1           765652
    zz-img.bin       1309756
    dflt-img.bin     1177004
    ap3xart.sys      641540
    syscfg_bak       26928
    syscfg           26928
    apcfg            2932
    zz-imgf.bin      1177004
    apcfg.bak        2932

2502656 bytes free

AP#
```

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access for RADIUS-aware devices to the network. An authentication server contains a database of credentials, such as users names and passwords, for each wireless client that requires access to the access point.

Command	Function	Mode	Page
radius-server address	Specifies the RADIUS server	GC	7-45
radius-server port	Sets the RADIUS server network port	GC	7-46
radius-server key	Sets the RADIUS encryption key	GC	7-47
radius-server retransmit	Sets the number of retries	GC	7-47
radius-server timeout	Sets the interval between sending authentication requests	GC	7-48
show radius	Shows the current RADIUS settings	Exec	7-48

radius-server address

This command specifies the primary and secondary RADIUS servers.

Syntax

radius-server address [secondary] <host_ip_address | host_name>

- **secondary** - Secondary server.
- *host_ip_address* - IP address of server.
- *host_name* - Host name of server. (Range: 1-20 characters)

Default Setting

None

Command Line Interface

Command Mode

Global Configuration

Example

```
AP(config)#radius-server address 192.168.1.25
AP(config)#
```

radius-server port

This command sets the RADIUS server network port.

Syntax

radius-server [**secondary**] **port** <*port_number*>

- **secondary** - Secondary server.
- *port_number* - RADIUS server UDP port used for authentication messages. (Range: 1024-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
AP(config)#radius-server port 181
AP(config)#
```


radius-server key

This command sets the RADIUS encryption key.

Syntax

radius-server [**secondary**] **key** <*key_string*>

- **secondary** - Secondary server.
- *key_string* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

DEFAULT

Command Mode

Global Configuration

Example

```
AP(config)#radius-server key green
AP(config)#
```

radius-server retransmit

This command sets the number of retries.

Syntax

radius-server [**secondary**] **retransmit** *number_of_retries*

- **secondary** - Secondary server.
- *number_of_retries* - Number of times the access point will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

3

Command Mode

Global Configuration

Command Line Interface

Example

```
AP(config)#radius-server retransmit 5
AP(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server.

Syntax

radius-server [**secondary**] **timeout** *number_of_seconds*

- **secondary** - Secondary server.
- *number_of_seconds* - Number of seconds the access point waits for a reply before resending a request. (Range: 1-60)

Default Setting

5

Command Mode

Global Configuration

Example

```
AP(config)#radius-server timeout 10
AP(config)#
```

show radius

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Exec

Example

```
AP#show radius

Radius Server Information
=====
IP                : 192.168.1.25
Port              : 181
Key               : *****
Retransmit        : 5
Timeout           : 10
=====

Radius Secondary Server Information
=====
IP                : 0.0.0.0
Port              : 1812
Key               : *****
Retransmit        : 3
Timeout           : 5
=====
AP#
```

Authentication

The access point supports IEEE 802.1x access control for wireless clients. This control feature prevents unauthorized access to the network by requiring a 802.1x client application to submit user credentials for authentication. Client authentication is then verified via by a RADIUS server using EAP (Extensible Authentication Protocol) before the access point grants client access to the network.

Command Line Interface

Client MAC addresses can also be used for authentication on the access point. For local MAC authentication, first define the default filtering policy using the address filter default command. Then enter the MAC addresses to be filtered, indicating if they are allowed or denied. For RADIUS MAC authentication, the MAC addresses and filtering policy must be configured on the RADIUS server.

Command	Function	Mode	Page
802.1x	Configures 802.1x as disabled, supported, or required	GC	7-51
802.1x broadcast-key-refresh-rate	Sets the interval at which the primary broadcast keys are refreshed for stations using 802.1x dynamic keying	GC	7-52
802.1x session-key-refresh-rate	Sets the interval at which unicast session keys are refreshed for associated stations using dynamic keying	GC	7-53
802.1x session-timeout	Sets the timeout after which a connected client must be re-authenticated	GC	7-54
802.1x supplicant	Sets the supplicant user name and password for the access point and enables the feature	GC	7-60
address filter default	Sets filtering to allow or deny listed addresses	GC	7-56
address filter entry	Enters a MAC address in the filter table	GC	7-57
address filter delete	Removes a MAC address from the filter table	GC	7-58
mac-authentication server	Sets address filtering to be performed with local or remote options	GC	7-59

Command	Function	Mode	Page
mac-authentication session-timeout	Sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database	GC	7-60
show authentication	Shows all 802.1x authentication settings, as well as the address filter table	Exec	7-60

802.1x

This command configures 802.1x as optionally supported or as required for wireless clients. Use the **no** form to disable 802.1x support.

Syntax

802.1x <supported | required>
no 802.1x

- **supported** - Authenticates clients that initiate the 802.1x authentication process. Uses standard 802.11 authentication for all others.
- **required** - Requires 802.1x authentication for all clients.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- When 802.1x is disabled, the access point does not support 802.1x authentication for any station. After successful 802.11 association, each client is allowed to access the network.

Command Line Interface

- When 802.1x is supported, the access point supports 802.1x authentication only for clients initiating the 802.1x authentication process (i.e., the access point does NOT initiate 802.1x authentication). For stations initiating 802.1x, only those stations successfully authenticated are allowed to access the network. For those stations not initiating 802.1x, access to the network is allowed after successful 802.11 association.
- When 802.1x is required, the access point enforces 802.1x authentication for all 802.11 associated stations. If 802.1x authentication is not initiated by the station, the access point will initiate authentication. Only those stations successfully authenticated with 802.1x are allowed to access the network.
- 802.1x does not apply to the 10/100Base-TX port.

Example

```
AP(config)#802.1x supported
AP(config)#
```

802.1x broadcast-key-refresh-rate

This command sets the interval at which the broadcast keys are refreshed for stations using 802.1x dynamic keying.

Syntax

802.1x broadcast-key-refresh-rate <rate>

rate - The interval at which the access point rotates broadcast keys. (Range: 0 - 1440 minutes)

Default Setting

0 (Disabled)

Command Mode

Global Configuration

Command Usage

- The access point uses EAPOL (Extensible Authentication Protocol Over LANs) packets to pass dynamic unicast session and broadcast keys to wireless clients. The **802.1x broadcast-key-refresh-rate** command specifies the interval after which the broadcast keys are changed. The **802.1x session-key-refresh-rate** command specifies the interval after which unicast session keys are changed.
- Dynamic broadcast key rotation allows the access point to generate a random group key and periodically update all key-management capable wireless clients.

Example

```
AP(config)#802.1x broadcast-key-refresh-rate 5
AP(config)#
```

802.1x session-key-refresh-rate

This command sets the interval at which unicast session keys are refreshed for associated stations using dynamic keying.

Syntax

802.1x session-key-refresh-rate *<rate>*

rate - The interval at which the access point refreshes a session key. (Range: 0 - 1440 minutes)

Default Setting

0 (Disabled)

Command Mode

Global Configuration

Command Usage

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Command Line Interface

Example

```
AP(config)#802.1x session-key-refresh-rate 5
AP(config)#
```

802.1x session-timeout

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form to disable 802.1x re-authentication.

Syntax

802.1x session-timeout <*seconds*>
no 802.1x session-timeout

seconds - The number of seconds. (Range: 0-65535)

Default

0 (Disabled)

Command Mode

Global Configuration

Example

```
AP(config)#802.1x session-timeout 300
AP(config)#
```


802.1x supplicant

This command sets the user name and password used for authentication of the access point when operating as a 802.1x supplicant and enables supplicant authentication. Use the **no** form to disable the feature.

Syntax

802.1x supplicant eth_password <password>

802.1x supplicant eth_user <username>

802.1x supplicant wds_password <port> <password>

802.1x supplicant wds_user <port> <username>

802.1x supplicant <eth | wds port>

no 802.1x supplicant <eth | wds port>

- **eth_password** - Specifies a password for authentication using the Ethernet port. (Range: 1-32 alphanumeric characters)
- **eth_user** - Specifies a username for authentication using the Ethernet port. (Range: 1-32 alphanumeric characters)
- **wds_password** - Specifies a password for authentication using the specified WDS port. (Range: 1-32 alphanumeric characters)
- **wds_user** - Specifies a username for authentication using the specified WDS port. (Range: 1-32 alphanumeric characters)
- **eth** - Enables 802.1X supplicant authentication using the Ethernet port.
- **wds** - Enables 802.1X supplicant authentication using the specified WDS port.
 - *port* - Specifies a WDS port number. (Range: 1-16 Master; 1 Slave)

Default

Disabled

Command Line Interface

Command Mode

Global Configuration

Command Usage

- Ethernet and WDS user names and passwords must be set before enabling the 802.1x supplicant feature for the specified port.
- The access point currently only supports EAP-MD5 CHAP for 802.1x supplicant authentication.

Example

```
AP(config)#802.1x supplicant wds_user 1 David
AP(config)#802.1x supplicant wds_password 1 ABC
AP(config)#802.1x supplicant wds 1
AP(config)#
```

address filter default

This command sets filtering to allow or deny listed MAC addresses.

Syntax

address filter default <allowed | denied>

- **allowed** - Only MAC addresses entered as “denied” in the address filtering table are denied.
- **denied** - Only MAC addresses entered as “allowed” in the address filtering table are allowed.

Default

allowed

Command Mode

Global Configuration

Example

```
AP(config)#address filter default denied
AP(config)#
```

Related Commands

address filter entry (page 7-57)
show authentication (page 7-60)

address filter entry

This command enters a MAC address in the filter table.

Syntax

address filter entry <mac-address> <allowed | denied>

- *mac-address* - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens; e.g., 00-90-D1-12-AB-89.)
- **allowed** - Entry is allowed access.
- **denied** - Entry is denied access.

Default

None

Command Mode

Global Configuration

Command Mode

- The access point supports up to 1024 MAC addresses.
- An entry in the address table may be allowed or denied access depending on the global setting configured for the **address entry default** command.

Command Line Interface

Example

```
AP(config)#address filter entry 00-70-50-cc-99-1a allowed
AP(config)#
```

Related Commands

address filter default (page 7-56)

show authentication (page 7-60)

address filter delete

This command deletes a MAC address from the filter table.

Syntax

address filter delete <mac-address>

mac-address - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens.)

Default

None

Command Mode

Global Configuration

Example

```
AP(config)#address filter delete 00-70-50-cc-99-1b
AP(config)#
```

Related Commands

show authentication (page 7-60)

mac-authentication server

This command sets address filtering to be performed with local or remote options. Use the **no** form to disable MAC address authentication.

Syntax

mac-authentication server [local | remote]

- **local** - Authenticate the MAC address of wireless clients with the local authentication database during 802.11 association.
- **remote** - Authenticate the MAC address of wireless clients with the RADIUS server during 802.1x authentication.

Default

local

Command Mode

Global Configuration

Example

```
AP(config)#mac-authentication server remote
AP(config)#
```

Related Commands

address filter entry (page 7-57)
radius-server address (page 7-45)
show authentication (page 7-60)

mac-authentication session-timeout

This command sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database. Use the **no** form to disable reauthentication.

Syntax

mac-authentication session-timeout <*seconds*>

seconds - Re-authentication interval. (Range: 0-65535)

Default

0 (disabled)

Command Mode

Global Configuration

Example

```
AP(config)#mac-authentication session-timeout 1
AP(config)#
```

show authentication

This command shows all 802.1x authentication settings, as well as the address filter table.

Command Mode

Exec

Example

```

AP#show authentication

Authentication Information
=====
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 1 secs
802.1x                        : SUPPORTED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1x Session Timeout Value   : 300 secs
Address Filtering               : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address      Status
-----
00-70-50-cc-99-1a  DENIED
00-70-50-cc-99-1b  ALLOWED
=====
AP#

```

WDS Commands

The commands described in this section are used to configure the Wireless Distribution System (WDS) forwarding table.

Command	Function	Mode	Page
wds channel	Selects the radio band to be used for bridge links	GC	7-62
wds mac-address	Configures MAC addresses of nodes in the wireless bridge network	GC	7-62
wds enable	Enables WDS forwarding for specific wireless port IDs	GC	7-63
show wds	Displays the current entries in the WDS forwarding table	Exec	7-64

Command Line Interface

wds channel

This command selects the radio band to be used for WDS forwarding (bridging).

Syntax

wds channel <a | g | none>

- **a** - Bridging is supported on the 802.11a 5 GHz band.
- **g** - Bridging is supported on the 802.11b/g 2.4 GHz band.
- **none** - Bridging is not supported for either band.

Default

802.11a

Command Mode

Global Configuration

Example

```
AP(config)#wds channel a
AP(config)#
```

wds mac-address

This command enters **Ethernet MAC Addresses** in the WDS forwarding table for each node in the wireless bridge network.

Syntax

wds mac-address <port-id> <mac-address>

- *port-id* - The wireless port number for the bridge link. (1 for Slave units; 1-16 for Master units)
- *mac-address* - The **Ethernet MAC Address** of the remote bridge unit for this link. (12 hexadecimal digits in the form "xx-xx-xx-xx-xx-xx")

Default

none

Command Mode

Global Configuration

Command Usage

- You can only configure one MAC address per wireless port ID.
- The Ethernet MAC address for each bridge unit is printed on the label on the back of the unit.
- When trying to connect to other bridges, please input the Ethernet MAC address

Example

```
AP(config)#wds mac-address 1 00-12-34-56-78-9a
AP(config)#
```

wds enable

This command enables WDS forwarding for a wireless port ID. Use the **no** form to disable WDS forwarding for a wireless port ID.

Syntax

[no] wds enable *<port-id>*

- *port-id* - The wireless port number for the link. (1 for Slave units; 1-16 for Master units)

Default

WDS forwarding disabled on all ports

Command Mode

Global Configuration

Example

```
AP(config)#wds enable 1
AP(config)#
```

Command Line Interface

show wds

This command displays the current entries in the WDS forwarding table.

Syntax

show wds

Command Mode

Exec

Example

AP#show wds

Outdoor_Mode		:	MASTER
=====			
Port ID		Status	Mac-Address
=====			
01		ENABLE	00-12-34-56-78-9A
02		ENABLE	00-1A-2B-3C-4D-5E
03		DISABLE	00-01-02-03-04-05
04		ENABLE	00-0E-87-3B-60-51
05		DISABLE	00-00-00-00-00-00
06		DISABLE	00-00-00-00-00-00
07		DISABLE	00-00-00-00-00-00
08		DISABLE	00-00-00-00-00-00
09		DISABLE	00-00-00-00-00-00
10		DISABLE	00-00-00-00-00-00
11		DISABLE	00-00-00-00-00-00
12		DISABLE	00-00-00-00-00-00
13		DISABLE	00-00-00-00-00-00
14		DISABLE	00-00-00-00-00-00
15		DISABLE	00-00-00-00-00-00
16		DISABLE	00-00-00-00-00-00
=====			
AP (config) #			

Bridge Commands

The commands described in this section are used to set the MAC address table aging time and spanning tree parameters for both the Ethernet and wireless interfaces.

Command	Function	Mode	Page
bridge timeout	Sets the aging time for the address table	GC	7-66
bridge stp-bridge spanning-tree	Enables the spanning tree protocol for the bridge	GC	7-66
bridge stp-bridge forward-time	Configures the spanning tree bridge forward time	GC	7-67
bridge stp-bridge hello-time	Configures the spanning tree bridge hello time	GC	7-68
bridge stp-bridge max-age	Configures the spanning tree bridge maximum age	GC	7-69
bridge stp-bridge priority	Configures the spanning tree bridge priority	GC	7-70
bridge stp-port path-cost	Configures the spanning tree path cost of a port	GC	7-71
bridge stp-port priority	Configures the spanning tree priority of a port	GC	7-72
bridge stp-port portfast	Sets a port to fast forwarding	GC	7-73
bridge stp-port spanning-disabled	Disables the spanning tree protocol on a port	GC	7-74
show bridge	Displays the current aging time settings	Exec	7-75

Command Line Interface

bridge timeout

This command sets the aging time for both the Ethernet port and the wireless interface.

Syntax

bridge timeout *<interface-id>* *<seconds>*

- *interface-id* - An identifier that specifies the interface. (0 for Ethernet, 2 for 802.11a wireless)
- *seconds* - The time to age out an address entry. (Range: 60-1800 seconds)

Default

Ethernet: 100

802.11a wireless: 1800

Command Mode

Global Configuration

Command Usage

- If the MAC address of an entry in the address table is not seen on the associated interface for longer than the aging time, the entry is discarded.

Example

```
AP(config)#bridge timeout 0 300
AP(config)#bridge timeout 2 1000
AP(config)#
```

bridge stp-bridge spanning-tree

Use this command to enable the Spanning Tree Protocol globally for the wireless bridge. Use the **no** form to disable it.

Syntax

bridge stp-bridge spanning-tree
no bridge stp-bridge spanning-tree

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the wireless bridge to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Protocol for the wireless bridge:

```
AP(config)#bridge stp-bridge spanning-tree
AP(config)#
```

bridge stp-bridge forward-time

Use this command to configure the spanning tree bridge forward time globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

bridge stp-bridge forward-time *seconds*

no bridge stp-bridge forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or $[(\text{max-age} / 2) + 1]$.

Command Line Interface

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
AP(config)#bridge stp-bridge forward-time 20
AP(config)#
```

bridge stp-bridge hello-time

Use this command to configure the spanning tree bridge hello time globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

bridge stp-bridge hello-time *time*

no bridge stp-bridge hello-time

time - Time in seconds. (Range: 1-10 seconds).

The maximum value is the lower of 10 or $[(\text{max-age} / 2) - 1]$.

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
AP(config)#bridge stp-bridge hello-time 5
AP(config)#
```

bridge stp-bridge max-age

Use this command to configure the spanning tree bridge maximum age globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

bridge stp-bridge max-age *seconds*

no bridge stp-bridge max-age

seconds - Time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or $[2 \times (\text{hello-time} + 1)]$.

The maximum value is the lower of 40 or $[2 \times (\text{forward-time} - 1)]$.

Default Setting

20 seconds

Command Mode

Global Configuration

Command Line Interface

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
AP(config)#bridge stp-bridge max-age 40
AP(config)#
```

bridge stp-bridge priority

Use this command to configure the spanning tree priority globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

bridge stp-bridge priority *priority*
no bridge stp-bridge priority

priority - Priority of the bridge. (Range: 0 - 65535)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
AP(config)#bridge stp-bridge priority 40000
AP(config)#
```

bridge stp-port path-cost

Use this command to configure the spanning tree path cost for the specified port. Use the **no** form to restore the default for the specified port.

Syntax

bridge stp-port path-cost <port> cost

no bridge stp-port path-cost <port>

- *port* - Specifies the port number on the wireless bridge. (Range: 0, Ethernet interface; 1-16 wireless interface)
- *cost* - The path cost for the port. (Range: 1-65535)

Default Setting

Ethernet interface – 19

Wireless interface – 40

Command Mode

Global Configuration

Command Line Interface

Command Usage

- This command is used by the Spanning Tree Protocol to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.

Example

```
AP(config)#bridge stp-port path-cost 1 50
AP(config)#
```

bridge stp-port priority

Use this command to configure the priority for the specified port.
Use the **no** form to restore the default for the specified port.

Syntax

bridge stp-port priority <port> priority
no bridge stp-port priority <port>

- *port* - Specifies the port number on the wireless bridge. (Range: 0, Ethernet interface; 1-16 wireless interface)
- *priority* - The priority for a port. (Range: 1-255)

Default Setting

128

Command Mode

Global Configuration

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Protocol. If the path cost for all ports on a wireless bridge are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
AP(config)#bridge stp-port priority 1 64
AP(config)#
```

Related Commands

bridge stp-port path-cost (page 7-71)

bridge stp-port portfast

Use this command to set an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

bridge stp-port portfast <port>

no bridge stp-port portfast <port>

port - Specifies the port number on the wireless bridge.
(Range: 0, Ethernet interface; 1-16 wireless interface)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.

Command Line Interface

- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node devices, and also overcome other STP related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)

Example

```
AP(config)#bridge stp-port portfast 15
AP(config)#
```

bridge stp-port spanning-disabled

This command disables the Spanning Tree Protocol for the specified interface. Use the **no** form to reenable the Spanning Tree Protocol for the specified interface.

Syntax

bridge stp-port spanning-disabled <port>
no bridge stp-port spanning-disabled <port>

port - Specifies the port number on the wireless bridge.
(Range: 0, Ethernet interface; 1-16 wireless interface)

Default Setting

Enabled

Command Mode

Global Configuration

Example

This example disables the Spanning Tree Protocol for port 5.

```
AP(config)#bridge stp-port spanning-disabled 5
AP(config)#
```

show bridge

This command displays aging time and spanning tree settings for the Ethernet and wireless interfaces.

Syntax

show bridge

Command Mode

Exec

Example

```
AP#show bridge

                        Bridge Information
=====
Media Type | Age Time(sec) |
=====
  Ethernet |    300        |
  WLAN_A   |   1000        |
=====

Bridge Id           : 32768.037fbef192
Root Bridge Id      : 32768.01f47483e2
Root Path Cost      : 25
Root Port Id        : 0
Bridge Status        : Enabled
Bridge Priority      : 32768
Bridge Hello Time    : 2 Seconds
Bridge Maximum Age   : 20 Seconds
Bridge Forward Delay: 15 Seconds
===== Port Summary
=====
Id| Priority | Path Cost | Fast Forward | Status |
State |
0   128      25           Enable    Enabled
Forwarding

AP#
```

Filtering Commands

The commands described in this section are used to control access to the management interface from the wireless interface and filter traffic using specific Ethernet protocol types.

Command	Function	Mode	Page
filter local-bridge	Disables communication between wireless clients	GC	7-76
filter ap-manage	Prevents access to the management interface over the wireless bridge link	GC	7-77
filter ethernet-type enable	Checks the Ethernet type for all incoming and outgoing Ethernet packets against the protocol filtering table	GC	7-78
filter ethernet-type protocol	Sets a filter for a specific Ethernet type	GC	7-79
show filter	Shows the filter configuration	Exec	7-80

filter local-bridge

This command disables communication between wireless clients. Use the **no** form to disable this filtering.

Syntax

filter local-bridge
no filter local-bridge

Default

Disabled

Command Mode

Global Configuration

Command Usage

This command can disable wireless-to-wireless communications between clients via the access point. However, it does not affect communications between wireless clients and the wired network.

Example

```
AP(config)#filter local-bridge
AP(config)#
```

Related Commands

filter ethernet-type enable (page 7-78)

filter ap-manage

This command prevents access to wireless bridge management from the wireless interface. Use the **no** form to disable this filtering.

Syntax

filter ap-manage
no filter ap-manage

Default

Disabled

Command Mode

Global Configuration

Example

```
AP(config)#filter ap-manage
AP(config)#
```

filter ethernet-type enable

This command checks the Ethernet type on all incoming and outgoing Ethernet packets against the protocol filtering table. Use the **no** form to disable this feature.

Syntax

filter ethernet-type enable
no filter ethernet-type enable

Default

Disabled

Command Mode

Global Configuration

Command Usage

This command is used in conjunction with the **filter ethernet-type protocol** command to determine which Ethernet protocol types are to be filtered.

Example

```
AP(config)#filter ethernet-type enable
AP(config)#
```

Related Commands

filter ethernet-type protocol (page 7-79)

filter ethernet-type protocol

This command sets a filter for a specific Ethernet type. Use the **no** form to disable filtering for a specific Ethernet type.

Syntax

filter ethernet-type protocol <protocol>

no filter ethernet-type protocol <protocol>

protocol - An Ethernet protocol type. (Options: ARP, RARP, Berkeley-Trailer-Negotiation, LAN-Test, X25-Level-3, Banyan, CDP, DEC XNS, DEC-MOP-Dump-Load, DEC-MOP, DEC-LAT, Ethertalk, Appletalk-ARP, Novell-IPX(old), Novell-IPX(new), EAPOL, Telxon-TXP, Aironet-DDP, Enet-Config-Test)

Default

None

Command Mode

Global Configuration

Command Usage

Use the **filter ethernet-type enable** command to enable filtering for Ethernet types specified in the filtering table, or the **no filter ethernet-type enable** command to disable all filtering based on the filtering table.

Example

```
AP(config)#filter ethernet-type protocol ARP
AP(config)#
```

Related Commands

filter ethernet-type enable (page 7-78)

Command Line Interface

show filters

This command shows the filter options and protocol entries in the filter table.

Command Mode

Exec

Example

```
AP#show filters

Protocol Filter Information
=====
AP Management           :ENABLED
Ethernet Type Filter    :ENABLED

Enabled Protocol Filters
-----
Protocol: ARP                               ISO: 0x0806
=====
AP#
```

PPPoE Commands

The commands described in this section configure PPPoE management tunnel connection parameters for the Ethernet port.

Command	Function	Mode	Page
ip pppoe	Enables PPPoE on the Ethernet interface	IC-E	7-81
pppoe ip allocation mode	Specifies how IP addresses for the PPPoE tunnel are configured on the interface	IC-E	7-82
pppoe ipcp dns	Negotiates DNS for the PPPoE tunnel	IC-E	7-83
pppoe lcp echo-interval	Sets LCP echo interval for the PPPoE tunnel	IC-E	7-84

Command	Function	Mode	Page
pppoe lcp echo-failure	Sets LCP echo timeout for the PPPoE tunnel	IC-E	7-85
pppoe local ip	Sets local IP address for the PPPoE tunnel	IC-E	7-86
pppoe remote ip	Sets remote IP address for the PPPoE tunnel	IC-E	7-86
pppoe username	Sets the user name for the PPPoE tunnel	IC-E	7-87
pppoe password	Sets the password for the PPPoE tunnel	IC-E	7-88
pppoe service-name	Sets the service name for the PPPoE tunnel	IC-E	7-89
pppoe restart	Restarts the PPPoE connection with updated parameters	IC-E	7-89
show pppoe	Shows information about the PPPoE configuration	PE	7-90

ip pppoe

This command enables Point-to-Point Protocol over Ethernet (PPPoE) on the Ethernet interface. Use the **no** form to disable PPPoE on the Ethernet interface.

Syntax

ip pppoe
no ip pppoe

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Line Interface

Command Usage

The access point uses a PPPoE connection, or tunnel, only for management traffic between the access point and a remote PPPoE server (typically at an ISP). Examples of management traffic that may initiated by the access point and carried over a PPPoE tunnel are RADIUS, Syslog, or DHCP traffic.

Example

```
AP# (if-ethernet) #ip pppoe
AP#
```

pppoe ip allocation mode

This command specifies how IP addresses for the PPPoE tunnel are configured on this interface.

Syntax

pppoe ip allocation mode {automatic | static}

- **automatic** - IP addresses are dynamically assigned by the ISP during PPPoE session initialization.
- **static** - Fixed addresses are assigned by the ISP for both the local and remote IP addresses.

Default Setting

automatic

Command Mode

Interface Configuration (Ethernet)

Command Usage

The IP address allocation mode depends on the type of service provided by the ISP. If automatic mode is selected, DHCP is used to allocate the IP addresses for the PPPoE connection. If static addresses have been assigned to by the ISP, these must be entered using the **pppoe local ip** and **pppoe remote ip** commands.

Example

```
AP#(if-ethernet)#pppoe ip allocation mode static
AP#
```

Related Commands

pppoe local ip (page 7-86)
pppoe remote ip (page 7-86)

pppoe ipcp dns

This command requests allocation of IP addresses for Dynamic Naming System (DNS) servers from the device at the remote end of the PPPoE tunnel.

Syntax

pppoe ipcp dns
no pppoe ipcp dns

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

DNS servers are used to translate host computer names into IP addresses. PPPoE clients can request a primary and secondary DNS server from the network connection device at the remote end of the PPPoE tunnel. This request is passed to the remote end during the IP Control Protocol (IPCP) negotiation phase during session initialization.

Example

```
AP#(if-ethernet)#pppoe ipcp dns
AP#
```

pppoe lcp echo-interval

This command sets the Link Control Protocol (LCP) echo interval for the PPPoE tunnel.

Syntax

pppoe lcp echo-interval *<interval>*

interval - The interval between sending echo requests.
(Range: 1-60 seconds)

Default Setting

10

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Echo requests are used to verify the integrity of the link through the PPPoE tunnel. Devices at either end of the link can issue an echo-request. Devices receiving an echo-request must return an echo-reply.
- If a link is busy with large data transfers, the echo-reply may not be issued in a timely manner causing the link to timeout. If you experience this kind of problem, try extending the echo interval or timeout.

Example

```
AP#(if-ethernet) #pppoe lcp echo-interval 30
AP#
```

Related Commands

pppoe lcp echo-failure (page 7-85)

pppoe lcp echo-failure

This command sets the Link Control Protocol (LCP) echo timeout for the PPPoE tunnel.

Syntax

pppoe lcp echo-failure <timeout>

timeout - The number of timeouts allowed. (Range: 1-10)

Default Setting

3

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Echo requests are used to verify the integrity of the link through the PPPoE tunnel. Devices at either end of the link can issue an echo-request. Devices receiving an echo-request must return an echo-reply.
- If a link is busy with large data transfers, the echo-reply may not be issued in a timely manner causing the link to timeout. If you experience this kind of problem, try extending the echo interval or timeout.

Example

```
AP#(if-ethernet)#pppoe lcp echo-failure 5
AP#
```

Related Commands

pppoe lcp echo-interval (page 7-84)

Command Line Interface

pppoe local ip

This command sets the local IP address for the PPPoE tunnel.

Syntax

pppoe local ip <ip-address>

ip-address - IP address of the local end of the PPPoE tunnel.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If the **pppoe ip allocation mode** is set to static, the local IP address must be entered with this command, and the remote IP address must be entered with the **pppoe remote ip** command.

Example

```
AP#(if-ethernet)#pppoe local ip 10.7.1.200
AP#
```

Related Commands

pppoe ip allocation mode (page 7-82)

pppoe remote ip (page 7-86)

pppoe remote ip

This command sets the remote IP address for the PPPoE tunnel.

Syntax

pppoe remote ip <ip-address>

ip-address - IP address of the remote end of the PPPoE tunnel.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If the **pppoe ip allocation mode** is set to static, the remote IP address must be entered with this command, and the local IP address must be entered with the **pppoe local ip** command.

Example

```
AP#(if-ethernet)#pppoe remote ip 192.168.1.20
AP#
```

Related Commands

pppoe ip allocation mode (page 7-82)

pppoe local ip (page 7-86)

pppoe username

This command sets the user name for the PPPoE tunnel.

Syntax

pppoe username <username>

username - User name assigned by the service provider.
(Range: 1-63 alphanumeric characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Line Interface

Command Usage

You must enter a user name with this command, and a password with the **pppoe password** command.

Example

```
AP#(if-ethernet) #pppoe username mike
AP#
```

Related Commands

pppoe password (page 7-88)

pppoe password

This command sets the password for the PPPoE tunnel.

Syntax

pppoe password <string>

string - Password assigned by the service provider.
(Range: 1-63 alphanumeric characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

You must enter a password with this command, and a user name with the **pppoe username** command.

Example

```
AP#(if-ethernet) #pppoe password 12345
AP#
```

Related Commands

pppoe username (page 7-87)

pppoe service-name

This command sets the service name for the PPPoE tunnel.

Syntax

pppoe service-name <*string*>

string - Service name assigned by the service provider.
(Range: 1-63 alphanumeric characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

The service name is normally optional, but may be required by some service providers.

Example

```
AP#(if-ethernet)#pppoe service-name classA
AP#
```

pppoe restart

This command restarts the PPPoE connection with updated parameters.

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command restarts PPPoE service using the most recently configured parameters.

Command Line Interface

Example

```
AP#(if-ethernet)#pppoe restart
AP#
```

show pppoe

This command shows information about the PPPoE configuration.

Command Mode

Privileged Exec

Example

```
AP#show pppoe

PPPoE Information
=====
State                : Link up
Username              : mike
Service Name          : classA
IP Allocation Mode    : Static
DNS Negotiation       : Enabled
Local IP              : 10.7.1.200
Echo Interval         : 30
Echo Failure          : 5
=====

AP#
```

Ethernet Interface Commands

The commands described in this section configure connection parameters for the Ethernet interface.

Command	Function	Mode	Page
interface ethernet	Enters Ethernet interface configuration mode	GC	7-91
dns primary-server	Specifies the primary name server	IC-E	7-92
dns secondary-server	Specifies the secondary name server	IC-E	7-92
ip address	Sets the IP address for the Ethernet interface	IC-E	7-93
ip dhcp	Submits a DHCP request for an IP address	IC-E	7-94
shutdown	Disables the Ethernet interface	IC-E	7-95
show interface ethernet	Shows the status for the Ethernet interface	Exec	7-96

interface ethernet

This command enters Ethernet interface configuration mode.

Syntax

interface ethernet

Default Setting

None

Command Mode

Global Configuration

Command Line Interface

Example

To specify the 10/100Base-TX network interface, enter the following command:

```
AP(config)#interface ethernet
AP(if-ethernet)#
```

dns server

This command specifies the address for the primary or secondary domain name server to be used for name-to-address resolution.

Syntax

dns primary-server <server-address>

dns secondary-server <server-address>

- **primary-server** - Primary server used for name resolution.
- **secondary-server** - Secondary server used for name resolution.
- *server-address* - IP address of domain-name server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The primary and secondary name servers are queried in sequence.

Example

This example specifies two domain-name servers.

```
AP(if-ethernet)#dns primary-server 192.168.1.55
AP(if-ethernet)#dns secondary-server 10.1.0.55
AP(if-ethernet)#
```

Related Commands

show interface ethernet (page 7-96)

ip address

This command sets the IP address for the (10/100Base-TX) Ethernet interface. Use the **no** form to restore the default IP address.

Syntax

ip address <*ip-address*> <*netmask*> <*gateway*>

no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- *gateway* - IP address of the default gateway

Default Setting

IP address: 192.168.2.2

Netmask: 255.255.255.0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- DHCP is enabled by default. To manually configure a new IP address, you must first disable the DHCP client with the **no ip dhcp** command.

Command Line Interface

- You must assign an IP address to this device to gain management access over the network or to connect the wireless bridge to existing IP subnets. You can manually configure a specific IP address using this command, or direct the device to obtain an address from a DHCP server using the **ip dhcp** command. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.

Example

```
AP(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
AP(if-ethernet)#ip address 192.168.1.2 255.255.255.0
192.168.1.253
AP(if-ethernet)#
```

Related Commands

ip dhcp (page 7-94)

ip dhcp

This command enables the access point to obtain an IP address from a DHCP server. Use the **no** form to restore the default IP address.

Syntax

ip dhcp
no ip dhcp

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must assign an IP address to this device to gain management access over the network or to connect the wireless bridge to existing IP subnets. You can manually configure a specific IP address using the **ip address** command, or direct the device to obtain an address from a DHCP server using this command.
- When you use this command, the wireless bridge will begin broadcasting DHCP client requests. The current IP address (i.e., default or manually configured address) will continue to be effective until a DHCP reply is received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (DHCP values can include the IP address, subnet mask, and default gateway.)

Example

```
AP(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
AP(if-ethernet)#ip dhcp
AP(if-ethernet)#
```

Related Commands

[ip address \(page 7-93\)](#)

shutdown

This command disables the Ethernet interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
no shutdown

Default Setting

Interface enabled

Command Line Interface

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command allows you to disable the Ethernet port due to abnormal behavior (e.g., excessive collisions), and reenale it after the problem has been resolved. You may also want to disable the Ethernet port for security reasons.

Example

The following example disables the Ethernet port.

```
AP(if-ethernet) #shutdown
AP(if-ethernet) #
```

show interface ethernet

This command displays the status for the Ethernet interface.

Syntax

show interface [ethernet]

Default Setting

Ethernet interface

Command Mode

Exec

Example

```
AP#show interface ethernet
Ethernet Interface Information
=====
IP Address           : 192.168.2.2
Subnet Mask          : 255.255.255.0
Default Gateway      : 192.168.1.253
Primary DNS          : 192.168.1.55
Secondary DNS        : 10.1.0.55
Admin status         : Up
Operational status   : Up
=====
AP#
```

Wireless Interface Commands

The commands described in this section configure connection parameters for the wireless interface.

Command	Function	Mode	Page
interface wireless	Enters wireless interface configuration mode	GC	7-99
description	Adds a description to the wireless interface	IC-W	7-99
ssid	Configures the service set identifier	IC-W	7-104
closed system	Prohibits access to clients without a pre-configured SSID	IC-W	7-101
speed	Configures the maximum data rate for transmitting unicast packets on the wireless interface	IC-W	7-101
channel	Configures the radio channel	IC-W	7-102
turbo	Configures the 802.11a radio to use a faster proprietary modulation mode	IC-W	7-103
beacon-interval	Configures the rate at which beacon signals are transmitted from the wireless bridge	IC-W	7-104

Command Line Interface

Command	Function	Mode	Page
dtim-period	Configures the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions	IC-W	7-104
fragmentation-length	Configures the minimum packet size that can be fragmented	IC-W	7-105
rts-threshold	Sets the packet size threshold at which an RTS must be sent to the receiving station prior to the sending station starting communications	IC-W	7-106
transmit-power	Adjusts the power of the radio signals transmitted from the wireless bridge	IC-W	7-107
max-association	Configures the maximum number of clients that can be associated with the access point radio at the same time	IC-W	7-108
authentication	Defines the 802.11 authentication type allowed by the access point	IC-W	7-109
encryption	Defines whether or not WEP or AES encryption is used to provide privacy for wireless communications	IC-W	7-110
key	Sets the keys used for WEP or AES encryption	IC-W	7-112
transmit-key	Sets the index of the key to be used for WEP encryption	IC-W	7-113
multicast-cipher	Defines the cipher algorithm used for multicasting	IC-W	7-114
wpa-clients	Defines whether WPA is required or optionally supported for client stations	IC-W	7-116
wpa-mode	Specifies dynamic keys or a pre-shared key	IC-W	7-117
wpa-preshared-key	Defines a WPA preshared-key value	IC-W	7-118
wpa-psk-type	Defines the type of the preshared-key	IC-W	7-120
shutdown	Disables the wireless interface	IC-W	7-120

Wireless Interface Commands

Command	Function	Mode	Page
show interface wireless	Shows the status for the wireless interface	Exec	7-120
show station	Shows the wireless clients associated with the access point	Exec	7-121

interface wireless

This command enters wireless interface configuration mode.

Syntax

interface wireless a

- **a** - 802.11a radio interface.
- **g** - 802.11g radio interface

Default Setting

None

Command Mode

Global Configuration

Example

To specify the wireless interface, enter the following command:

```
AP(config)#interface wireless a
AP(if-wireless a)#
```

description

This command adds a description to the wireless interface. Use the **no** form to remove the description.

Syntax

description <string>

no description

string - Comment or a description for this interface.
(Range: 1-80 characters)

Command Line Interface

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Example

```
AP(config)#interface wireless a
AP(if-wireless a)#description RD-AP#3
AP(if-wireless a)#
```

ssid

This command configures the service set identifier (SSID).

Syntax

ssid <*string*>

string - The name of a basic service set supported by the access point. (Range: 1 - 32 characters)

Default Setting

SMC

Command Mode

Interface Configuration (Wireless)

Command Usage

Clients that want to connect to the wireless network via an access point must set their SSIDs to the same as that of the access point.

Example

```
AP(if-wireless g)#ssid RD-AP#3
AP(if-wireless g)#
```

closed-system

This command closes access to clients without a pre-configured SSID. Use the **no** form to disable this feature.

Syntax

closed-system
no closed-system

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

When SSID Broadcast is disabled, the access point will not include its SSID in beacon messages. Nor will it respond to probe requests from clients that do not include a fixed SSID.

Example

```
AP(if-wireless g)#closed-system
AP(if-wireless g)#
```

speed

This command configures the maximum data rate for transmitting unicast packets on the wireless interface.

Syntax

speed <speed>

speed - Maximum access speed allowed for remote bridges.
(Options: 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;
802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps)

Default Setting

54 Mbps

Command Line Interface

Command Mode

Interface Configuration (Wireless)

Command Usage

The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance.

Example

```
AP(if-wireless a) #speed 6
AP(if-wireless a) #
```

channel

This command configures the radio channel through which the local wireless bridge communicates with remote bridges.

Syntax

channel <*channel* | **auto**>

- **channel** - Manually sets the radio channel used for communications with remote bridges. (Range: 802.11a - 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165 for normal mode, and 42, 50, 58, 152, 160 for turbo mode; 802.1g - 1 to 14)
- **auto** - Automatically selects an unoccupied channel (if available). Otherwise, the lowest channel is selected.

Default Setting

Automatic channel selection

Command Mode

Interface Configuration (Wireless)

Command Usage

The available channel settings are limited by local regulations, which determine the number of channels that are available.

Example

```
AP(if-wireless a)#channel 36
AP(if-wireless a)#
```

turbo

This command sets the wireless bridge to an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless - 802.11a)

Command Usage

- The normal 802.11a wireless operation mode provides connections up to 54 Mbps. Turbo Mode is an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps. Enabling Turbo Mode allows the wireless bridge to provide connections up to 108 Mbps.
- In normal mode, the wireless bridge provides a channel bandwidth of 20 MHz, and supports the maximum number of channels permitted by local regulations (e.g., 11 channels for the United States). In Turbo Mode, the channel bandwidth is increased to 40 MHz to support the increased data rate. However, this reduces the number of channels supported (e.g., 5 channels for the United States).

Example

```
AP(if-wireless a)#turbo
AP(if-wireless a)#
```

Command Line Interface

beacon-interval

This command configures the rate at which beacon signals are transmitted from the wireless bridge.

Syntax

beacon-interval *<interval>*

interval - The rate for transmitting beacon signals.
(Range: 20-1000 milliseconds)

Default Setting

100

Command Mode

Interface Configuration (Wireless)

Command Usage

The beacon signals allow remote bridges to maintain contact with the local wireless bridge. They may also carry power-management information.

Example

```
AP(if-wireless a)#beacon-interval 150
AP(if-wireless a)#
```

dtim-period

This command configures the rate at which remote bridges in sleep mode must wake up to receive broadcast/multicast transmissions.

Syntax

dtim-period *<interval>*

interval - Interval between the beacon frames that transmit broadcast or multicast traffic. (Range: 1-255 beacon frames)

Default Setting

2

Command Mode

Interface Configuration (Wireless)

Command Usage

- The Delivery Traffic Indication Map (DTIM) packet interval value indicates how often the MAC layer forwards broadcast/multicast traffic. This parameter is necessary to wake up remote bridges that are using Power Save mode.
- The DTIM is the interval between two synchronous frames with broadcast/multicast information. The default value of 2 indicates that the wireless bridge will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon.
- Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing remote bridges in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by remote bridges in Power Save mode, but delays the transmission of broadcast/multicast frames.

Example

```
AP(if-wireless a)#dtim-period 100
AP(if-wireless a)#
```

fragmentation-length

This command configures the minimum packet size that can be fragmented when passing through the wireless bridge.

Syntax

fragmentation-length <length>

length - Minimum packet size for which fragmentation is allowed. (Range: 256-2346 bytes)

Command Line Interface

Default Setting

2346

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the packet size is smaller than the preset Fragment size, the packet will not be segmented.
- Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames.

Example

```
AP(if-wireless a)#fragmentation-length 512
AP(if-wireless a)#
```

rts-threshold

This command sets the packet size threshold at which a Request to Send (RTS) signal must be sent to the receiving remote bridge prior to the sending bridge starting communications.

Syntax

rts-threshold <threshold>

threshold - Threshold packet size for which to send an RTS.
(Range: 0-2347 bytes)

Default Setting

2347

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the threshold is set to 0, the wireless bridge always sends RTS signals. If set to 2347, the wireless bridge never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.
- The wireless bridge sends RTS frames to a receiving remote bridge to negotiate the sending of a data frame. After receiving an RTS frame, the remote bridge sends a CTS frame to notify the local bridge that it can start sending data.
- Wireless bridges contending for the wireless medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node” problem.

Example

```
AP(if-wireless a)#rts-threshold 256
AP(if-wireless a)#
```

transmit-power

This command adjusts the power of the radio signals transmitted from the wireless bridge.

Syntax

transmit-power <signal-strength>

signal-strength - Signal strength transmitted from the wireless bridge. (Options: full, half, quarter, eighth, min)

Command Line Interface

Default Setting

full

Command Mode

Interface Configuration (Wireless)

Command Usage

- The “min” keyword indicates minimum power.
- The longer the transmission distance, the higher the transmission power required. Power selection is not just a trade off between coverage area and maximum data rates. You also have to ensure that high strength signals do not interfere with the operation of other radio devices in your area.

Example

```
AP(if-wireless a)#transmit-power half
AP(if-wireless a)#
```

max-association

This command configures the maximum number of clients that can be associated with the access point at the same time.

Syntax

max-association <count>

count - Maximum number of associated stations.
(Range: 0-64)

Default Setting

64 (per radio)

Command Mode

Interface Configuration (Wireless)

Example

```
AP(if-wireless g) #max-association 32
AP(if-wireless g) #
```

authentication

This command defines the 802.11 authentication type allowed by the access point.

Syntax

authentication <open | shared>

- **open** - Accepts the client without verifying its identity using a shared key.
- **shared** - Authentication is based on a shared key that has been distributed to all stations.

Default Setting

open

Command Mode

Interface Configuration (Wireless)

Command Usage

- Shared key authentication can only be used when WEP is enabled with the **encryption** command, and at least one static WEP key has been defined with the **key** command.
- When using WPA or 802.1x for authentication and dynamic keying, the access point must be set to **open**.

Example

```
AP(if-wireless g) #authentication shared
AP(if-wireless g) #
```

Related Commands

encryption (page 7-110)
key (page 7-112)

encryption

This command defines whether WEP or AES encryption is used to provide privacy for wireless communications. Use the **no** form to disable encryption.

Syntax

encryption {**wep** <*key-length*> | **wdsaes** <**alphanumeric** | **hex**>}

no encryption

- **wep** - The keyword that enables WEP encryption.
 - *key-length* - Size of encryption key. (Options: 64, 128, or 152 bits)
- **wdsaes** - The keyword that enables 128-bit AES encryption.
 - **alphanumeric** - Specifies an encryption key entered as an alphanumeric string.
 - **hex** - Specifies an encryption key entered as hexadecimal digits.

Default Setting

disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

- Wired Equivalent Privacy (WEP) and Advanced Encryption Standard (AES) are implemented in this device to prevent unauthorized access to your network. For more secure data transmissions, enable WEP or AES encryption with this command, and set at least one key with the **key** command.

Wireless Interface Commands

- AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 standard.
- The WEP settings must be the same on all bridges in your wireless network.
- The WEP encryption length specified in the **encryption** command and the **key** command must match.
- The AES keys must match for each wireless bridge link pair.
- The AES key type value entered using the **key** command must be the same as the type specified in the **encryption** command.
- Note that encryption protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Example

```
AP(if-wireless a)#encryption wep 128
AP(if-wireless a)#
```

Related Commands

key (page 7-112)

Command Line Interface

key

This command sets the keys used for WEP and AES encryption. Use the **no** form to delete a configured key.

Syntax

key {**wep** <*index size type wep-value*> | **wdsaes** <*port-id aes-value*>}

no key {**wep** <*index*> | **wdsaes**}

- **wep** - The keyword that specifies a WEP encryption key.
 - *index* - Key index. (Range: 1-4)
 - *size* - Key size. (Options: 64, 128, or 152 bits)
 - *type* - Input format. (Options: ASCII, HEX)
 - *wep-value* - The WEP key string. For ASCII input, use 5/13/16 alphanumeric characters for 64/128/152 bit keys. For HEX input, use 10/26/32 hexadecimal digits for 64/128/152 bit keys.
- **wdsaes** - The keyword that specifies an AES encryption key
 - *port-id* - The ID for the wireless port on the bridge. For Slave units, the ID is 1. For Master units, the ID can be from 1 to 16.
 - *aes-value* - The AES key string. For alphanumeric input, use 8 to 31 characters. For hexadecimal input, use exactly 32 digits.

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Command Usage

- To enable WEP encryption, use the **encryption** command to specify the key type and length, and use the **key** command to configure at least one key.

- To enable AES encryption, use the **encryption** command to specify the key type, and use the **key** command to configure a key for each wireless port.
- If WEP is enabled, all units in the wireless bridge network must be configured with the same keys.
- The WEP key length specified in the **encryption** command and the **key** command must match.
- The WEP key index, length and type configured on the local wireless bridge must match those configured on other wireless bridges.
- If AES is enabled, each wireless bridge link in the network must be configured to use the same AES key
- The AES key type value entered using the **key** command must be the same as the type specified in the **encryption** command.

Example

```
AP(if-wireless a)#key wep 1 64 ascii 12345
AP(if-wireless a)#key wep 2 64 ascii abcde
AP(if-wireless a)#
```

Related Commands

encryption (page 7-110)

transmit-key

This command sets the index of the WEP key to be used for encrypting data frames broadcast or multicast from the wireless bridge.

Syntax

transmit-key <index>

index - Key index. (Range: 1-4)

Default Setting

1

Command Line Interface

Command Mode

Interface Configuration (Wireless)

Command Usage

- If you use WEP key encryption, the wireless bridge uses the transmit key to encrypt multicast and broadcast data signals that it sends to other nodes. Other keys can be used for decryption of data from other nodes.

Example

```
AP(if-wireless a)#transmit-key 2
AP(if-wireless a)#
```

multicast-cipher

This command defines the cipher algorithm used for broadcasting and multicasting when using Wi-Fi Protected Access (WPA) security.

Syntax

multicast-cipher <AES | TKIP | WEP>

- **AES** - Advanced Encryption Standard
- **TKIP** - Temporal Key Integrity Protocol
- **WEP** - Wired Equivalent Privacy

Default Setting

WEP

Command Mode

Interface Configuration (Wireless)

Command Usage

- WPA enables the access point to support different unicast encryption keys for each client. However, the global encryption key for multicast and broadcast traffic must be the same for all clients. This command sets the encryption type that is supported by all clients.
- If any clients supported by the access point are not WPA enabled, the multicast-cipher algorithm must be set to WEP.
- WEP is the first generation security protocol used to encrypt data crossing the wireless medium using a fairly short key. Communicating devices must use the same WEP key to encrypt and decrypt radio signals. WEP has many security flaws, and is not recommended for transmitting highly sensitive data.
- TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.
- TKIP defends against attacks on WEP in which the unencrypted initialization vector in encrypted packets is used to calculate the WEP key. TKIP changes the encryption key on each packet, and rotates not just the unicast keys, but the broadcast keys as well. TKIP is a replacement for WEP that removes the predictability that intruders relied on to determine the WEP key.
- AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 standard.

Example

```
AP(if-wireless g)#multicast-cipher TKIP
AP(if-wireless g)#
```

wpa-clients

This command defines whether Wi-Fi Protected Access (WPA) is required or optionally supported for client stations.

Syntax

wpa-clients <required | supported>

- **required** - Supports only clients using WPA.
- **supported** - Support clients with or without WPA.

Default Setting

Supported

Command Mode

Interface Configuration (Wireless)

Command Usage

Wi-Fi Protected Access (WPA) provides improved data encryption, which was weak in WEP, and user authentication, which was largely missing in WEP. WPA uses the following security mechanisms.

Enhanced Data Encryption through TKIP

WPA uses Temporal Key Integrity Protocol (TKIP). TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.

Enterprise-level User Authentication via 802.1x and EAP

To strengthen user authentication, WPA uses 802.1x and the Extensible Authentication Protocol (EAP). Used together, these protocols provide strong user authentication via a central RADIUS authentication server that authenticates each user on the network before they join it. WPA also employs “mutual authentication” to prevent a wireless client from accidentally joining a rogue network.

Example

```
AP(if-wireless g)#wpa-client required
AP(if-wireless g)#
```

Related Commands

wpa-mode (page 7-117)

wpa-mode

This command specifies whether Wi-Fi Protected Access (WPA) is to use 802.1x dynamic keys or a pre-shared key.

Syntax

wpa-mode <dynamic | pre-shared-key>

- **dynamic** - WPA with 802.1x dynamic keys.
- **pre-shared-key** - WPA with a pre-shared key.

Default Setting

dynamic

Command Mode

Interface Configuration (Wireless)

Command Usage

- When the WPA mode is set to “dynamic,” clients are authenticated using 802.1x via a RADIUS server. Each client has to be WPA-enabled or support 802.1x client software. A RADIUS server must also be configured and be available in the wired network.
- In the dynamic mode, keys are generated for each wireless client associating with the access point. These keys are regenerated periodically, and also each time the wireless client is re-authenticated.
- When the WPA mode is set to “pre-shared-key,” the key must first be generated and distributed to all wireless clients before they can successfully associate with the access point.

Command Line Interface

Example

```
AP(if-wireless g)#wpa-mode pre-shared-key  
AP(if-wireless g)#
```

Related Commands

wpa-clients (page 7-116)

wpa-preshared-key (page 7-118)

wpa-preshared-key

This command defines a Wi-Fi Protected Access (WPA) preshared-key.

Syntax

wpa-preshared-key <type> <value>

- *type* - Input format. (Options: ASCII, HEX)
- *value* - The key string. For ASCII input, use 5/13 alphanumeric characters for 64/128 bit strings. For HEX input, use 10/26 hexadecimal digits for 64/128 bit strings.

Command Mode

Interface Configuration (Wireless)

Command Usage

- To support Wi-Fi Protected Access (WPA) for client authentication, use the **wpa-clients** command to specify the authentication type, use the **wpa-mode** command to specify pre-shared-key mode, and use this command to configure one static key.
- If WPA is used with pre-shared-key mode, all wireless clients must be configured with the same pre-shared key to communicate with the access point.

Example

```
AP(if-wireless g)#wpa-preshared-key ASCII agoodsecret
AP(if-wireless g)#
```

Related Commands

wpa-clients (page 7-116)

wpa-mode (page 7-117)

wpa-psk-type

This command defines the Wi-Fi Protected Access (WPA) preshared-key type.

Syntax

wpa-psk-type <type>

type - Input format. (Options: Alphanumeric, HEX)

Default Setting

HEX

Command Mode

Interface Configuration (Wireless)

Example

```
AP(if-wireless a)#wpa-preshared-key ASCII agoodsecret
AP(if-wireless a)#
```

Related Commands

wpa-preshared-key (page 7-118)

Command Line Interface

shutdown

This command disables the wireless interface. Use the **no** form to restart the interface.

Syntax

shutdown
no shutdown

Default Setting

Interface enabled

Command Mode

Interface Configuration (Wireless)

Example

```
AP(if-wireless a)#shutdown
AP(if-wireless a)#
```

show interface wireless

This command displays the status for the wireless interface.

Syntax

show interface wireless <a | g>

- **a** - 802.11a radio interface.
- **g** - 802.11g radio interface

Command Mode

Exec

Example

```
AP#show interface wireless a

Wireless Interface Information
=====
-----Identification-----
Description                : Enterprise 802.11a Wireless
  Outdoor Bridge/AP
Service Type               : WDS Bridge
SSID                      : DualBandOutdoor
Turbo Mode                 : OFF
Channel                   : 36
Status                    : Enable
-----802.11 Parameters-----
Transmit Power             : FULL (15 dBm)
Max Station Data Rate      : 54Mbps
Fragmentation Threshold    : 2346 bytes
RTS Threshold              : 2347 bytes
Beacon Interval            : 100 TUs
DTIM Interval              : 2 beacons
Maximum Association        : 64 stations
-----Security-----
Encryption                 : 128-BIT AES ENCRYPTION
AES Key type               : Alphanumeric
=====
AP#
```

show station

This command shows the wireless clients associated with the access point.

Command Mode

Exec

Command Line Interface

Example

```
AP#show station

Station Table Information
=====
802.11a Channel : 56

No 802.11a Channel Stations.
802.11g Channel : 11
802.11g Channel Station Table
Station Address   : 00-04-E2-41-C2-9D VLAN ID: 0
Authenticated Associated Forwarding KeyType
TRUE             TRUE      TRUE      NONE
Counters:pkts    Tx        /        Rx    bytes    Tx        /        Rx
                  4/              0          1440/              0
Time:Associated  LastAssoc  LastDisAssoc LastAuth
                143854      0              0              0
=====
AP#
```

IAPP Commands

The command described in this section enables the protocol signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points. In other words, the 802.11f protocol can ensure successful roaming between access points in a multi-vendor environment.

iapp

This command enables the protocol signaling required to hand over wireless clients roaming between different 802.11f-compliant access points. Use the **no** form to disable 802.11f signaling.

Syntax

iapp
no iapp

Default

Enabled

Command Mode

Global Configuration

Command Usage

The current 802.11 standard does not specify the signaling required between access points in order to support clients roaming from one access point to another. In particular, this can create a problem for clients roaming between access points from different vendors. This command is used to enable or disable 802.11f handover signaling between different access points, especially in a multi-vendor environment.

Example

```
AP(config)#iapp
AP(config)#
```

VLAN Commands

The wireless bridge can enable the support of VLAN-tagged traffic passing between the wireless interface and the wired network.

When VLAN support is enabled, the wireless bridge tags traffic passing to the wired network with the assigned native VLAN ID (a number between 1 and 64). Traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.

When VLAN support is disabled, the wireless bridge does not tag traffic passing to the wired network and ignores the VLAN tags on any received frames.

Command Line Interface

Note: Before enabling VLANs on the wireless bridge, you must configure the connected LAN switch port to accept tagged VLAN packets with the wireless bridge's native VLAN ID. Otherwise, connectivity to the wireless bridge will be lost when you enable the VLAN feature.

The VLAN commands supported by the wireless bridge are listed below.

Command	Function	Mode	Page
vlan	Enables a single VLAN for all traffic	GC	7-124
native-vlanid	Configures the native VLAN for the access point	GC	7-125

vlan

This command enables VLANs for all traffic. Use the **no** form to disable VLANs.

Syntax

vlan enable
no vlan

Default

Disabled

Command Mode

Global Configuration

Command Description

- Changing the VLAN status of the wireless bridge forces a system reboot.
- When VLANs are enabled, the wireless bridge tags frames received from wireless interface with the configured native VLAN ID.
- Traffic entering the Ethernet port must be tagged with a VLAN ID that matches the wireless bridge's native VLAN ID.

Example

```
AP(config)#vlan enable
Reboot system now? <y/n>: y
```

Related Commands

native-vlanid (page 7-125)

native-vlanid

This command configures the native VLAN ID for the wireless bridge.

Syntax

native-vlanid <vlan-id>

vlan-id - Native VLAN ID. (Range: 1-64)

Default Setting

1

Command Mode

Global Configuration

Command Usage

When VLANs are enabled, the wireless bridge tags traffic passing to the wired network with the configured native VLAN ID (a number between 1 and 64).

Example

```
AP(config)#native-vlanid 3
AP(config)#
```

Related Commands

vlan (page 7-124)

Command Line Interface

Appendix A

Troubleshooting

Check the following items before you contact local Technical Support.

1. If wireless bridge units do not associate with each other, check the following:
 - Check the power injector LED for each bridge unit to be sure that power is being supplied
 - Be sure that antennas in the link are properly aligned.
 - Be sure that channel settings match on all bridges
 - If encryption is enabled, ensure that all bridge links are configured with the same encryption keys.
2. If you experience poor performance (high packet loss rate) over the wireless bridge link:
 - Check that the range of the link is within the limits for the antennas used.
 - Be sure that antennas in the link are properly aligned.
 - Check that there is an unobstructed radio line-of-sight between the antennas.
 - Be sure there is no interference from other radio sources. Try setting the bridge link to another radio channel.
 - Be sure there is no other radio transmitter too close to either antenna. If necessary, move the antennas to another location.

Troubleshooting

3. If the wireless bridge cannot be configured using Telnet, a web browser, or SNMP software:
 - Be sure to have configured the wireless bridge with a valid IP address, subnet mask and default gateway.
 - Check that you have a valid network connection to the wireless bridge and that the Ethernet port or the wireless interface has not been disabled.
 - If you are connecting to the wireless bridge through the wired Ethernet interface, check the network cabling between the management station and the wireless bridge.
 - If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted (i.e, four sessions). Try connecting again at a later time.
4. If all other recovery measures fail, and the wireless bridge is still not functioning properly, take any of these steps:
 - Reset the wireless bridge's hardware using the CLI, web interface, or through a power reset.
 - Reset the wireless bridge to its default configuration.
5. If you forgot or lost the password:
 - Contact Technical Support.

Appendix B

Specifications

General Specifications

Maximum Channels (Outdoor)

802.11a:

US & Canada: 9 (normal mode), 3 (turbo mode)

Japan: 4 (normal mode), 1 (turbo mode)

ETSI: 11 channels (normal mode), 4 (turbo mode)

Taiwan: 4 (normal mode), 1 (turbo mode)

802.11g:

FCC/IC: 1-11

ETSI: 1-13

France: 1-7

MKK: 1-14

Taiwan: 1-11

Data Rates

802.11a:

Normal Mode: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel

Turbo Mode: 12, 18, 24, 36, 48, 72, 96, 108 Mbps per channel

802.11g:

6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel

802.11b:

1, 2, 5.5, 11 Mbps per channel

Maximum Clients

64 for the radio interface set to access point mode

Specifications

Modulation Types

802.11a: BPSK, QPSK, 16-QAM, 64-QAM

802.11g: CCK, BPSK, QPSK, OFDM

802.11b: CCK, BPSK, QPSK

Network Configuration

Bridge Mode:

Point-to-point and point-to-multipoint

Access Point Mode:

Infrastructure

Operating Frequency

802.11a:

5.15 ~ 5.25 GHz (lower band) US/Canada

5.25 ~ 5.35 GHz (middle band) US/Canada

5.725 ~ 5.825 GHz (upper band) US/Canada

5.25 ~ 5.35 GHz (middle band) Taiwan

5.725 ~ 5.825 GHz (high band) Taiwan

802.11b/g:

2.4 ~ 2.4835 GHz (US, Canada, ETSI)

2.4 ~ 2.497 GHz (Japan)

2.400 ~ 2.4835 GHz (Taiwan)

Power Injector

Input: 100-240 VAC, 47-63 Hz, 1.5 A

Output: 48 VDC, 1.2 A

Bridge Power (DC)

Input voltage: 48 volts, 1.2 A, 30 watts maximum

Physical Size

19.8 x 19.8 x 6.33 cm (7.8 x 7.8 x 2.49 in)

Weight

4.8 kg (10.58 lbs)

Network Management

Web-browser, Telnet, SNMP

Temperature

Operating: -33 to 55 °C (-27.4 to 131 °F)

Storage: -40 to 80 °C (-40 to 176 °F)

Humidity

5% to 95% (non-condensing)

EMC Compliance (Class B)

FCC Class B (US)

RTTED 1999/5/EC

DGT (Taiwan)

Radio Signal Certification

FCC Part 15 15.407(b) (5 GHz)

FCC Part 15.247 (2.4 GHz)

EN 300.328, EN 302.893

EN 300 826, EN 301.489-1, EN 301.489-17

ETSI 300.328; ETS 300 826 (802.11b)

Safety

CSA/NTRL (CSA 22.2 No. 950 & UL 1950)

Standards

IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX,

IEEE 802.11a, b, g

Antenna Specifications

17 dBi Integrated Panel

Frequency Range

5.150 - 5.850 GHz

Gain

17 dBi

VSWR

1.8 : 1 max

Polarization

Linear, vertical/horizontal

HPBW

Horizontal: 20°

Vertical: 22°

Front-to-Back Ratio

>25 dB

Power Handling

10 W (cw)

Impedance

50 Ohms

Connector

SMA female

Antenna Specifications

17 dBi Integrated Panel Antenna Link Budget (5.825 GHz, Cable Loss 1 dB, Fade Margin 5 dB)			
Modulation/Rates	Transmit Power (dBm)	Receive Sensitivity (dBm)	Maximum Range (km) with 17 dBi Panel*
Normal Mode			
BPSK (6 Mbps)	20	-88	15.4
BPSK (9 Mbps)	20	-87	14.7
QPSK (12 Mbps)	20	-86	14.0
QPSK (18 Mbps)	20	-84	12.8
16 QAM (24 Mbps)	20	-81	11.1
16 QAM (36 Mbps)	20	-76	6.5
64 QAM (48 Mbps)	18	-71	2.9
64 QAM (54 Mbps)	17	-68	1.8
Turbo Mode			
BPSK (12 Mbps)	20	-85	13.4
BPSK (18 Mbps)	20	-84	12.8
QPSK (24 Mbps)	20	-83	12.2
QPSK (36 Mbps)	20	-81	11.1
16 QAM (48 Mbps)	20	-78	8.2
16 QAM (72 Mbps)	20	-73	4.6
64 QAM (96 Mbps)	18	-68	2.1
64 QAM (108 Mbps)	17	-65	1.3

* The maximum range calculated with a 17 dBi panel antenna at the far end of the link.
The maximum transmit power (hence range) may be lowered by regulatory (FCC etc) EIRP (effective isotropic radiated power) limits.

Specifications

Appendix C

Cables and Pinouts

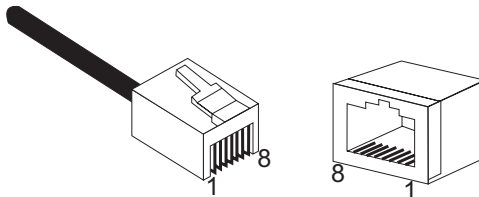
Twisted-Pair Cable Assignments

For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Caution: Each wire pair must be attached to the RJ-45 connectors in a specific orientation.

Caution: DO NOT plug a phone jack connector into a power injector RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



10/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100-ohm Category 5 or better cable for 100 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 Input port on the power injector is wired with MDI pinouts. This means that you must use crossover cables for connections to PCs or servers, and straight-through cable for connections to switches or hubs. However, when connecting to devices that support automatic MDI/MDI-X pinout configuration, you can use either straight-through or crossover cable.

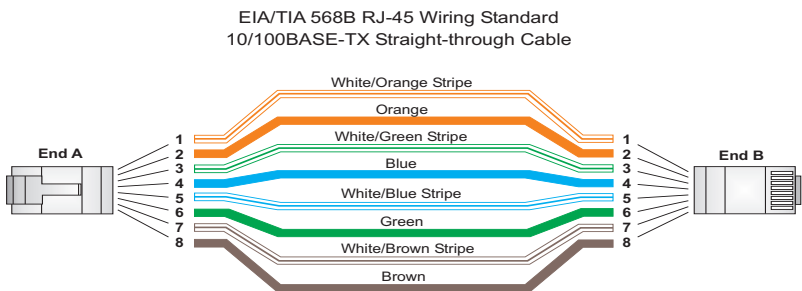
10/100BASE-TX MDI and MDI-X Port Pinouts		
Pin	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)
4,5,7,8	Not used	Not used

Note: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

Twisted-Pair Cable Assignments

Straight-Through Wiring

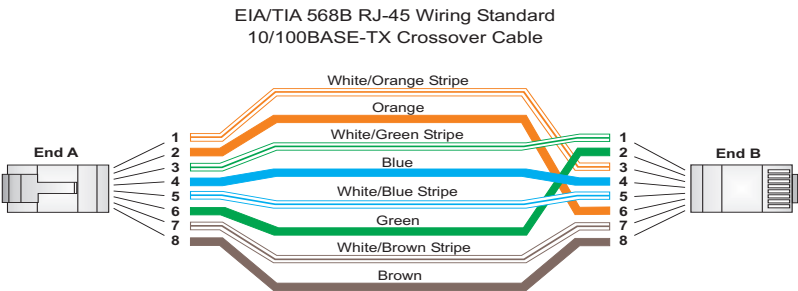
Because the 10/100 Mbps Input port on the power injector uses an MDI pin configuration, you must use “straight-through” cable for network connections to hubs or switches that only have MDI-X ports. However, if the device to which you are connecting supports automatic MDI/MDI-X operation, you can use either “straight-through” or “crossover” cable.



Crossover Wiring

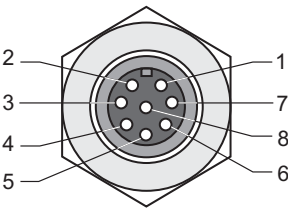
Because the 10/100 Mbps port on the power injector uses an MDI pin configuration, you must use “crossover” cable for network connections to PCs, servers or other end nodes that only have MDI ports. However, if the device to which you are connecting supports automatic MDI/MDI-X operation, you can use either “straight-through” or “crossover” cable.

Cables and Pinouts



8-Pin DIN Connector Pinout

The Ethernet cable from the power injector connects to an 8-pin DIN connector on the wireless bridge. This connector is described in the following figure and table.



8-Pin DIN Ethernet Port Pinout	
Pin	Signal Name
1	Transmit Data plus (TD+)
2	Transmit Data minus (TD-)
3	Receive Data plus (RD+)
4	+48 VDC power

8-Pin DIN Connector Pinout

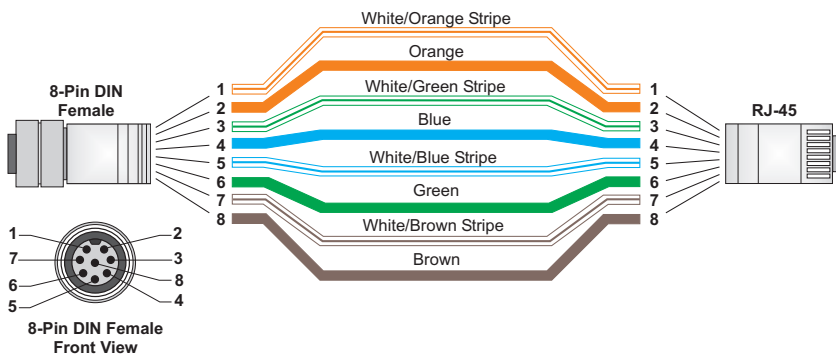
8-Pin DIN Ethernet Port Pinout	
Pin	Signal Name
5	+48 VDC power
6	Receive Data minus (RD-)
7	Return power
8	Return power

Note: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

8-Pin DIN to RJ-45 Cable Wiring

To construct an extended Ethernet cable to connect from the power injector’s RJ-45 Output port to the wireless bridge’s 8-pin DIN connector, follow the wiring diagram below. Use Category 5 or better UTP or STP cable, maximum length 100 m (328 ft), and be sure to connect all four wire pairs.

Note: To construct a reliable Ethernet cable, always use the proper tools or ask a professional cable supplier to construct the cable.



Cables and Pinouts

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

Advanced Encryption Standard (AES)

An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

Authentication

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Backbone

The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Glossary

Basic Service Set (BSS)

A set of 802.11-compliant stations and an access point that operate as a fully-connected wireless network.

Beacon

A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance.

dBm

The unit dBm refers to a precise measure of power based upon the decibel scale, but referenced to the milliwatt: i.e. $1 \text{ dBm} = .001 \text{ Watt}$. The dBm is often used to describe absolute power level where the point of reference is 1 milliwatt.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between the access point and clients can use encryption to protect from interception and eavesdropping.

Ethernet

A popular local area data communications network, which accepts transmission from computers and terminals.

File Transfer Protocol (FTP)

A TCP/IP protocol used for file transfer.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive all data over the World Wide Web.

Internet Control Message Protocol (ICMP)

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

IEEE 802.11a

A wireless standard that supports high-speed communications in the 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard supports data rates of 6, 12, 24, and 54 Mbps.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Glossary

Open System

A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM/ allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

RTS Threshold

Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this "Hidden Node Problem." If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

Service Set Identifier (SSID)

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

Session Key

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Shared Key

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Wired Equivalent Privacy (WEP)

WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

Glossary

Index

A

- Advanced Encryption Standard *See* AES
- AES 6-82
 - configuring 6-68
- AES, configuring 6-66, 7-110
- authentication 6-16, 7-109
 - configuring 6-16, 7-109
 - MAC address 6-18, 7-56, 7-57
 - type 5-10, 6-72, 7-101

B

- Basic Service Set *See* BSS
- beacon
 - interval 6-59, 7-104
 - rate 6-59, 7-104
- BOOTP 7-93, 7-94
- BPDU 6-48
- BSS 2-3

C

- cable
 - assignments C-1
 - crossover C-3
 - straight-through C-3
- channel 6-58, 7-102
- channels, maximum B-1
- Clear To Send *See* CTS
- CLI 7-1
 - command modes 7-6
- clients, maximum B-1
- closed system 7-101
- command line interface *See* CLI
- community name, configuring 6-30, 7-34
- community string 6-32, 7-34

- configuration settings, saving or restoring 6-36, 7-41
- configuration, initial setup 5-1
- country code
 - configuring 5-2, 7-16
- crossover cable C-3
- CSMA/CA 1-2
- CTS 6-60, 7-107

D

- data rate, options B-1
- default settings 1-10
- device status, displaying 6-87, 7-22
- DHCP 5-8, 6-7, 6-8, 7-93, 7-94, 7-95
- DNS 6-9, 7-92
- Domain Name Server *See* DNS
- downloading software 6-34, 7-41
- DTIM 6-59, 7-104
- Dynamic Host Configuration Protocol
 - See* DHCP

E

- EAP 6-80, 7-116
- encryption 6-66, 6-72, 6-74, 6-81, 7-110
- Ethernet
 - port 1-5
- event logs 6-92, 7-27
- Extensible Authentication Protocol
 - See* EAP

F

- factory defaults
 - restoring 6-36, 7-13
- fast forwarding, STP 6-52

Index

- filter 6-26, 7-56
 - address 6-16, 7-56
 - between wireless clients 6-28, 7-76
 - local bridge 6-28, 7-76
 - local or remote 6-16, 7-59
 - management access 6-28, 7-77
 - protocol types 6-28, 7-78
 - VLANs 6-26, 7-123
- firmware
 - displaying version 6-35, 7-23
 - upgrading 6-34, 6-36, 7-41
- fragmentation 7-105

G

- gateway address 5-3, 6-9, 7-2, 7-93

H

- hardware version, displaying 7-23

I

- IAPP 7-122
- IEEE 802.11a 1-2, 6-56, 7-99
 - configuring interface 6-57, 7-99
 - maximum data rate 6-59, 7-101
 - radio channel 6-58, 7-102
- IEEE 802.11b 6-56
- IEEE 802.11f 7-122
- IEEE 802.11g 6-56
 - configuring interface 6-63
 - maximum data rate 6-64, 7-101
 - radio channel 6-63, 7-102
- IEEE 802.1x 6-80, 7-49
 - configuring 6-16, 6-19, 7-49
- initial setup 5-1
- installation
 - hardware 4-1

- IP address
 - BOOTP/DHCP 7-93, 7-94
 - configuring 5-3, 5-8, 6-7, 7-93, 7-94

L

- log
 - messages 6-39, 6-92, 7-24
 - server 6-38, 7-24
- login
 - web 5-4
- logon authentication
 - RADIUS client 6-21, 7-45

M

- MAC address, authentication 6-18, 7-56, 7-57
- maximum data rate 6-59, 6-64, 7-101
 - 802.11a interface 6-59, 7-101
 - 802.11g interface 6-64, 7-101
- MDI, RJ-45 pin configuration 1-6
- multicast cipher 6-83, 7-114

N

- network topologies
 - infrastructure 2-3
 - infrastructure for roaming 2-4

O

- OFDM 1-2
- open system 5-10, 6-72, 7-101
- operating frequency B-2

P

- package checklist 1-2

password
 configuring 6-33, 7-20
 management 6-33, 7-20
 PoE 4-8
 specifications B-2
 port priority
 STA 7-72
 Power over Ethernet *See* PoE
 power supply, specifications B-2
 PSK 6-81, 7-117

R

radio channel
 802.11a interface 6-58, 7-102
 802.11g interface 6-63, 7-102
 configuring 5-6
 RADIUS 6-10, 6-80, 7-45
 RADIUS, logon authentication 6-21, 7-45
 Remote Authentication Dial-in User Service *See* RADIUS
 Request to Send *See* RTS
 reset 6-36, 7-13
 reset button 1-6, 6-36
 resetting the access point 6-36, 7-13
 restarting the system 6-36, 7-13
 RSSI BNC 1-7
 RTS
 threshold 6-60, 7-106

S

security, options 6-72
 session key 6-19, 6-20, 7-53
 shared key 5-10, 6-67, 6-76, 7-112
 Simple Network Management Protocol *See* SNMP
 Simple Network Time Protocol *See* SNTP

SNMP 6-30, 7-34
 community name 6-30, 7-34
 community string 7-34
 enabling traps 6-31, 7-36
 trap destination 6-31, 7-37
 trap manager 6-31, 7-37
 SNTP 6-40, 6-41, 7-29
 enabling client 6-41, 7-30
 server 6-41, 7-29
 software
 displaying version 6-34, 6-87, 7-23
 downloading 6-36, 7-41
 specifications B-1
 SSID 7-100
 configuring 5-6
 STA
 global settings,
 configuring 7-66-??
 interface settings 7-71-??
 path cost 7-71
 port priority 7-72
 startup files, setting 7-40
 station status 6-90, 7-121
 status
 displaying device status 6-87, 7-22
 displaying station status 6-90, 7-121
 STP
 fast forwarding 6-52
 straight-through cable C-3
 system clock, setting 6-41, 7-31
 system log
 enabling 6-38, 7-24
 server 6-38, 7-24
 system software, downloading from
 server 6-34, 7-41

T

Telnet
 for managenet access 7-1

Index

Temporal Key Integrity Protocol *See* TKIP

time zone 6-41, 7-32

TKIP 6-81, 7-114

transmit power, configuring 6-59, 7-107

trap destination 6-31, 7-37

trap manager 6-31, 7-37

troubleshooting A-1

U

upgrading software 6-34, 7-41

user name, manager 6-33, 7-19

user password 6-33, 7-19, 7-20

V

VLAN

configuration 6-26, 7-124

native ID 6-26, 7-125

W

WEP 6-66, 6-74, 7-110

configuring 6-66, 6-74, 7-110

shared key 6-67, 6-76, 7-112

Wi-Fi Protected Access *See* WPA

Wired Equivalent Protection *See* WEP

WPA 6-80, 7-117

authentication over 802.11x 6-83, 7-116

pre-shared key 6-83, 6-84, 7-118, 7-119

WPA, pre-shared key *See* PSK

SMC2888W-S
SMC2888W-M